

Niina Syrjärinne

## **HENKILÖTIETOLAINSÄÄDÄNNÖN VAIKUTUKSET TYÖSUHTEESEEN PAI- KANNUSRATKAISUJA HYÖDYNNETTÄESSÄ**

# **HENKILÖTIETOLAINSÄÄDÄNNÖN VAIKUTUKSET TYÖSUHTEESEEN PAI- KANNUSRATKAISUJA HYÖDYNNETTÄESSÄ**

Niina Syrjärinne  
Opinnäytetyö  
Syksy 2018  
Liiketalous  
Oulun ammattikorkeakoulu

## TIIVISTELMÄ

Oulun ammattikorkeakoulu

Liiketalouden koulutusohjelma, Oikeuden ja hallinnon suuntautumisvaihtoehto

---

Tekijä: Niina Syrjärinne

Opinnäytetyön nimi: Henkilötietolainsäädännön vaikutukset työsuhteeseen paikannusratkaisuja hyödynnettäessä

Työn ohjaaja: Lea Isopoussu-Koponen

Työn valmistumislukukausi ja -vuosi: Syksy 2018

Sivumäärä: sivut + liitteet  
(61+ 3)

---

Tässä opinnäytetyössä tarkastellaan henkilötietolainsäädännön vaikutuksia työsuhteeseen paikannusratkaisuja hyödynnettäessä. Tarkoituksena on selvittää, miten Euroopan tietosuoja-asetus vaikuttaa teknisten valvontamenetelmien käyttöön työpaikoilla sekä millaisia lainsäädännöllisiä haasteita paikannusratkaisujen hyödyntäminen aiheuttaa. Lisäksi tarkoituksena on selvittää työntekijöiden suhtautumista tekniseen valvontaan työpaikalla ja heidän yksityisyyden suojaa koskeviin kysymyksiin.

Toimeksiantajana toimii Solita Oy, joka on suomalainen teknologia-, strategia- ja designyritys. Solitan palvelutarjoamaan kuuluu muun muassa IoT-ratkaisujen kehittäminen. Tämä kattaa datan keruun koneista ja laitteista, tiedon analysoinnin ja hyödyntämisen sekä uudet digitaaliset palvelut ja paikantamiseen liittyvät ratkaisut.

Opinnäytetyön tutkimusmenetelminä ovat lainoppi sekä laadullinen tutkimus, joka on toteutettu teemahaastatteluin erilaisissa tehtävissä toimiville työntekijöille sekä työnantajille keväällä 2018. Lisäksi osa opinnäytetyöstä on toteutettu toiminnallisena opinnäytetyönä siten, että opinnäytetyön tuloksena suunniteltiin toimeksiantajan käyttöön huoneentaulu. Huoneentaulu käsittelee paikantamisratkaisuja suunniteltaessa huomioon otettavia asioita. Keskeisimpiä lähteitä ovat Euroopan tietosuoja-asetus, laki yksityisyyden suojasta työelämässä sekä eri ministeriöiden antamat raportit ja ohjeet. Pääpaino on Euroopan tietosuoja-asetuksessa, joka tuli sovellettavaksi 25.5.2018. Kirjoittamishetkellä Suomen kansallinen lainsäädäntö on muutostilassa, joten lähdeaineistona on käytetty laajasti lainvalmisteluasiakirjoja sekä eri tahojen lausuntoja ja raportteja.

Johtopäätöksenä voidaan todeta, että Euroopan tietosuoja-asetus ei ota suoraan kantaa työntekijöiden paikantamiseen tai paikantamiseen ylipäätään. Paikantamisratkaisuja hyödynnettäessä kertyy kuitenkin henkilötiedoiksi luokiteltavia tietoja, joiden käsittelyä Euroopan tietosuoja-asetus sääntelee. Lainsäädännön voidaan kuitenkin tässä vaiheessa katsoa olevan monilta osin vielä hyvin tulkinnanvaraista, mikä aiheuttaa usein epävarmuutta yritysten toiminnassa. Tehdyn haastattelututkimuksen perusteella työntekijöiden voidaan katsoa suhtautuvan pääsääntöisesti positiivisesti työnantajan suorittamaan tekniseen valvontaan ja uusiin kokeiluihin, kunhan sille on riittävät perusteet.

---

Asiasanat: Henkilötietojen suoja, henkilötietolainsäädäntö, paikannus, yksityisyyden suoja työelämässä, yksityisyys, teollinen internet

## ABSTRACT

Oulu University of Applied Sciences

Degree programme in Business Economics, option of Law and Administration

---

Author: Niina Syrjärinne

Title of thesis: The Impact of personal data legislation on employment relationship when using positioning solutions

Supervisor: Lea Isopoussu-Koponen

Term and year when the thesis was submitted: Autumn 2018    Number of pages: 61+3

---

This thesis examines the impact of personal data legislation on employment relationship when using positioning solutions. The purpose of the thesis is to explore how the General Data Protection Regulation in the EU affects the use of technical control methods at workplaces and what kind of legislative challenges it may cause. In addition, the goal is to determine the employee's attitudes towards technical control at workplaces and their privacy issues.

The client company of the thesis is Solita Oy which is a Finnish digital transformation company. Solita's supply of services ranges from gathering data from various IT solutions and analyzing and utilizing this data. They also cover new digital and positioning services. The service selection more over includes developing IoT solutions.

The research method of this thesis was qualitative research, which was carried out in form of theme interviews. The interviewees were selected from different companies and the choice was based on the client's recommendations. This thesis was also partially practice based as the result of the thesis was a poster to cater the client's needs.

The theoretical background of the thesis consisted of general data protection regulation, personal information legislation, government proposals, solutions of different instances, instructions, articles and legal literature. At the time of writing this thesis, the Finnish national legislation was in a state of change, thus reports, articles and preparatory documents were the key source.

It can be deduced from the results of the study that the General Data Protection Regulation does not really take a stand when it comes to using positioning solutions. However, when using positioning solutions, the result may be such personal data which is covered by the Data Protection Regulation. However, this legislation can still be considered to be very open to interpretation which often causes uncertainty in business. Based on the theme interviews, the employees can be considered positively oriented to employer's technical supervision and new experiments if there are relevant grounds for doing so.

---

Keywords: personal data protection, personal information legislation, positioning solutions, privacy, privacy protection at work

# SISÄLLYS

1	JOHDANTO .....	9
2	TEOLLINEN INTERNET .....	11
2.1	Kuka omistaa datan ja tiedon? .....	13
2.2	Teollinen internet ja henkilötiedot .....	14
2.3	Teollinen internet ja tietoturva .....	15
2.4	Teollinen internet ja lainsäädäntö .....	16
3	YKSITYISYYS JA HENKILÖTIETOJEN SUOJA .....	18
4	HENKILÖTIETOJEN KÄSITTELY .....	21
4.1	Euroopan tietosuoja-asetus .....	21
4.1.1	Merkittävimmät muutokset .....	22
4.1.2	Henkilötietojen käsittelyä koskevat periaatteet tietosuoja-asetuksessa .....	23
4.1.3	Rekisteröidyn oikeudet .....	25
4.2	Tietosuojalaki .....	26
5	HENKILÖTIETOJEN KÄSITTELY TYÖSUHTEESSA .....	28
5.1	Paikka- ja sijaintitiedot .....	29
5.2	Työntekijän paikantamisen edellytykset .....	29
5.3	Välitön ja välillinen paikantaminen .....	30
5.4	Solita sisätilapaikannus Proof of concept (POC) .....	32
5.5	Yhteistoimintamenettely .....	33
6	TUTKIMUS .....	37
6.1	Tutkimusmenetelmät .....	37
6.2	Toteutus .....	37
6.3	Laaduntarkkailu ja luotettavuus .....	38
6.4	Huoneentaulun suunnittelu ja toteutus .....	39
7	TUTKIMUSTULOKSET .....	40
7.1	Suhtautuminen tekniseen valvontaan ja paikantamiseen .....	41
7.2	Paikantamisratkaisujen hyödyt ja haitat .....	43
7.3	Yksityisyys .....	45
7.4	Informointi .....	47
7.5	Paikantamiseen liittyvä lainsäädäntö .....	49
8	JOHTOPÄÄTÖKSET .....	52

9	POHDINTA.....	54
	LÄHTEET.....	57
	LIITTEET .....	27

## LYHENTEET

BYOD	Bring your own device
EIS	Euroopan ihmisoikeussopimus. Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi. 4.11.1950. (SopS 18-19/1990)
EOA	Eduskunnan oikeusasiamiehen ratkaisu
EU	Euroopan unioni
HE 125/2003 vp.	Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräksi siihen liittyviksi laeiksi
HE 309/1993 vp.	Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta
HE 75/2000vp.	Hallituksen esitys eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräksi siihen liittyviksi laeiksi
HE 9/2018 vp.	Hallituksen esitys Eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.
HeTiL	Henkilötietolaki 1999/523
IoT	Internet of Things, Teollinen internet
KP-sopimus	Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus ja siihen liittyvä valinnainen pöytäkirja yksilövalituksista.
LiVL	Liikenne- ja viestintävaliokunta
Paikkatietolaki	Laki paikkatietoinfrastruktuurista 421/2009
PatL	Patenttilaki 1967/550
PeVM25/1994	Eduskunnan perustuslakivaliokunnan mietintö n:o 25 hallituksen esityksestä perusoikeus-säännösten muuttamisesta HE 309/1993 vp
PL	Suomen perustuslaki 721/1999

POC	Proof of Concept
RL	Rikoslaki 1889/39
SEUT	Sopimus Euroopan unionin toiminnasta
TekijäL	Tekijänoikeuslaki 1961/404
Tietosuoja-asetus	EPNAs (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (GDPR) 27.4.2016
TSL	Työsopimuslaki
TYK	Laki sähköisen viestinnän palveluista
YksTL	Laki yksityisyyden suojasta työelämässä
YTL	Laki yhteistoiminnasta yrityksissä 2007/334
WP29-työryhmä	EU:n kansallisista tietosuojaviranomaisista koostuva työryhmä, joka julkaisee tietosuoja-asetuksen tulkintaa koskevia ohjeita



# 1 JOHDANTO

Viime vuosina tietomassat ovat kasvaneet valtavasti ja kasvavat edelleen myös tulevaisuudessa. Digitalisaation ja teknisen kehityksen edetessä tiedon kokonaishallinnan merkitys korostuu entisestään. Uusien teknologioiden hyödyntämiseen liittyy riskejä, jotka johtuvat esimerkiksi siitä, että tulevaisuudessa käsittelemme enenevässä määrin tietoa, jonka synnyttävät erilaiset laitteet ja sensorit. Tekninen kehitys tuo mukanaan haasteita yrityksille myös lainsäädännön näkökulmasta ja henkilötietojen käsittelyyn liittyvät oikeudet ja velvollisuudet nousevat aiempaa tärkeämpään rooliin.

Opinnäytetyön tarkoituksena on tutkia kuinka Euroopan yleinen tietosuoja-asetus vaikuttaa työntekijöiden paikantamiseen ja henkilötietojen keräämiseen, millaisia muita lainsäädännöllisiä haasteita paikantamiseen työpaikoilla voi liittyä ja millainen paikantaminen on ylipäätään työpaikalla mahdollista. Lisäksi tavoitteena on selvittää työntekijöiden suhtautumista paikantamiseen sekä työntekijöiden ja työnantajien saamia hyötyjä paikantamisratkaisusta.

Opinnäytetyön toimeksiantajana toimii Solita Oy, joka on noin 650 henkeä työllistävä suomalainen teknologia-, strategia- ja designyritys. Työ on toteutettu osittain toiminnallisena opinnäytetyönä siten, että sen tuloksena on luotu paikantamiseen liittyvä huoneentaulu (liite 3). Solitan palvelutarjoamaan kuuluu IoT-ratkaisujen kehittäminen sekä itse liiketoiminnan muovaaminen ja transformatio. Ratkaisut kattavat muun muassa datan keruun koneista ja laitteista, tiedon analysoinnin ja hyödyntämisen sekä uudet digitaaliset palvelut ja paikantamiseen liittyvät ratkaisut. Näitä palveluita tarjotessa tietosuoja ja yksityisyys ovat keskeisessä roolissa. Huoneentaulun on tarkoituksena toimia toimeksiantajan apuna asiakkuuksissa.

Sen lisäksi, että opinnäytetyö on toteutettu osittain toiminnallisena opinnäytetyönä, tutkimusmenetelmänä toimii laadullinen eli kvalitatiivinen tutkimus. Laadullinen tutkimus on toteutettu teemahaastatteluin. Haastattelujen avulla on pyritty vastaamaan jo aiemmin mainittuihin tutkimuskysymyksiin, jotka koskevat työntekijöiden subjektiivisia kokemuksia paikantamiseen liittyen sekä siitä saatavia hyötyjä. Lisäksi opinnäytetyössä on käytetty lainopillista tutkimusta. Aineistona on käytetty pääasiassa voimassa olevaa lainsäädäntöä, kirjoittamishetkellä vanhentumassa olevaa lainsäädäntöä, esitöitä sekä erilaisia ministeriöiden raportteja ja lausuntoja. Oikeuskirjallisuutta ja oikeustapauksia on ollut aiheen ajankohtaisuudesta johtuen saatavilla vain vähän.

Keskeisimpiä lähteitä opinnäytetyössä ovat Euroopan tietosuoja-asetus, laki yksityisyyden suojasta työelämässä sekä eri ministeriöiden antamat raportit ja ohjeet. Pääpaino on Euroopan tietosuoja-asetuksessa, joka tuli sovellettavaksi 25.5.2018. Kirjoittamishetkellä Suomen kansallinen lainsäädäntö on muutostilassa, joten lähdeaineistona on käytetty laajasti lainvalmisteluasiakirjoja sekä eri tahojen lausuntoja ja raportteja.

Tutkimusongelmaa on lähestytty opinnäytetyössä avaamalla aluksi käsitettä teollista internet yleisemmällä tasolla, koska paikannusratkaisuissa käytetään hyväksi erilaisia ihmisiin ja esineisiin kiinnitettäviä sensoreita. Lisäksi tarkastellaan teollisen internettiin liittyvän lainsäädännön nykytilaa sekä teollisen internetin, henkilötietojen keräämisen ja tietoturvan haasteita. Myös teollisen internetin synnyttämän tiedon ja datan omistajuuden pohdinta on keskeinen osa lainsäädännöllisiä haasteita, jotka syntyvät sensoreiden lisääntyessä yhteiskunnassa.

Kolmannessa luvussa on käsitelty tarkemmin yksityisyyttä sekä henkilötietojen suojaa. Neljäs ja viides luku käsittelevät henkilötietojen käsittelyä niin yleisesti kuin työsuhteessakin. Euroopan tietosuoja-asetus on keskeisin henkilötietojen käsittelyä koskeva säädös, joten raportissa on keskitytty erityisesti sen tuomiin muutoksiin, periaatteisiin ja rekisteröidyn oikeuksiin. Lisäksi on käsitelty kirjoittamishetkellä valmisteilla olevaa uutta tietosuojalakia. Raportin kuudennessa luvussa on esitelty toimeksiantajan tiloissa tapahtunutta paikannusdemoa ja seitsemännessä ja kahdeksannessa luvussa haastattelututkimusta.

Raportin loppupuolella luvuissa yhdeksän ja kymmenen on esitelty johtopäätökset ja pohdinta. Johtopäätöksissä analysoidaan haastattelutuloksia ja pohdinnassa raportin onnistumista sekä luotettavuutta. Pohdinnassa tuodaan esille myös kirjoittajan omia näkemyksiä ja pohditaan mahdollisia jatkotutkimusaiheita. Aivan raportin lopussa on lähteet sekä liitteinä teemahaastatteluissa käytetyt kysymykset ja toimeksiantajalle laadittu huoneentaulu.

## 2 TEOLLINEN INTERNET

Teollinen internet, josta käytetään myös nimitystä esineiden internet (Internet of Things, IoT), tarkoittaa ilmiötä, jossa verkkoon kytkettyjen laitteiden määrä lisääntyy. Nimestään huolimatta teollisessa internetissä ei ole kyse pelkästään teollisuuden internetistä. (Collin & Saarelainen, 30.)

Teollisessa internetissä sensorit, koneet, prosessit ja palvelut tuottavat jatkuvasti tietoa, jota jalostamalla voidaan ennakoita ja automatisoida työvaiheita. Kuluttajien näkökulmasta tämä helpottaa arkea, koska kaikilla esineillä ja asioilla on digitaalinen tunniste, jonka avulla niitä voidaan optimoida kuluttajille. Optimointi voi tarkoittaa esimerkiksi paremman käyttäjäkokemuksen luomista tai palveluilla voidaan parantaa kuluttajan terveyden edistämistä. Teollisen internetin suurin potentiaali liittyykin siihen, miten yksittäiset koneet ja laitteet toimivat yhteen ja kuinka se hyödyttää käyttäjää. (Collin, Halén, Juhanko, Jurvansuu, Koivisto, Kortelainen, Simons, Tuominen & Uusitalo. 2015, 10.)

Teollista internettiä on sanottu yhdeksi tämän hetken suurimmista murroksia. Niin Suomessa kuin muuallakin maailmassa haetaan uutta kasvua ja kilpailukykyä teollisen internetin hyödyntämisen kautta. Teollinen internet on nimetty yhdeksi valtioneuvoston kärkiteemoista ja Valtioneuvosto on toteuttanut myös selvitystyön teemalla ”Suomalainen Teollinen Internet – haasteesta mahdollisuudeksi”. (Collin ym. 2015, 3.)

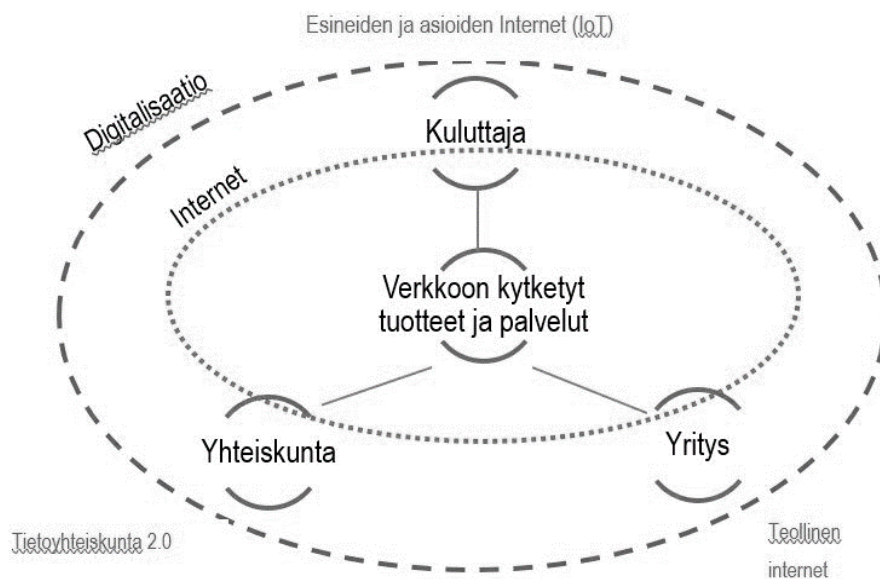
Collin ja Saarelainen ovat esittäneet teollisen internetin elementeiksi älykkäät koneet, kehittynyt analytiikka sekä ihmiset työssä. Collinin mukaan koneet, laitteet ja verkostot varustetaan kehittyneillä antureilla, kontrolleilla ja ohjelmistoilla. Fysiikkaan perustuva analytiikka, ennustavat algoritmit, automaatio ja toimialan tuntemus yhdistyvät. Tämän lisäksi ihmiset saavat ajasta ja paikasta riippumatta tukea tehdäkseen älykkäämpiä päätöksiä, palvellakseen paremmin ja toimiakseen turvallisemmin. (Collin & Saarelainen 2016, 22.)

Valtioneuvoston selvitys- ja tutkimustoiminta raportin mukaan, Suomi – teollisen internetin pilaakso, digitaalisuuden ja teollisen Internetin sekä niiden yhteisvaikutusten luoma murros on nähtävä positiivisena mahdollisuutena kasvattaa yhteiskunnan hyvinvointia ja tuottavuutta. Niiden avulla pystytään luomaan uusia työpaikkoja sekä puitteet uusille investoinneille sekä toimintaedellytyksille. (Collin ym. 2015, 3.)

Teollinen Internet on osa uutta digitalisaation muutosaaltoa, jossa verkkoon kytketyt tuotteet ja palvelut mahdollistavat tuotteiden ja palveluiden käytönaikaisen sitoutuneen pääoman ja tiedon hyödyntämisen älykkäällä tavalla. Se tuo muutoksia yritysten tuottavuuteen, johtamisen käytäntöihin, liiketoimintamalleihin sekä yleiseen kilpailuun uusista markkinoista ja asiakkuuksista. (Collin ym.2015, 10.)

Raportissa on esitelty myös käsite Tietoyhteiskunta 2.0. Tällä käsiteellä tarkoitetaan ilmiötä, jossa kansalainen on kytketty osaksi kansallista digitaalista palveluarkkitehtuuria. Kaikilla toimijoilla on digitaalinen tunniste, jonka avulla niille voidaan tarjota optimoituja palveluja. Suomessa kaikilla on oikeus ja mahdollisuus hyödyntää ja osallistua kansalaisille tarjottaviin digitaalisiin palveluihin koko Euroopan alueella. Nämä palvelut ovat siirtymässä kokonaisuudessaan digitaalisiksi internetiin. (Collin ym. 2015, 11.)

Tätä yhteiskunnan, yritysten sekä kuluttajien muodostamaa kokonaisuutta voidaan kuvata seuraavanlaisella kuviolla



KUVIO 1: Yhteiskunnan, kuluttajien ja yritysten muodostama kokonaisuus. (Mukaillen Collin ym. 2015, 11.)

Nämä kolme tahoa ovat yhdistymässä yhdeksi suuremmaksi kokonaisuudeksi, jossa verkkoon kytketyt laitteet ja niihin liittyvät erilaiset ohjelmisto-, sovellus- ja sisältökaupat sekä pilvipalvelut toimivat yhteisenä keskeisenä alustana yhteiskunnalle, teollisuudelle ja kuluttajalle (Collin ym. 2015, 12).

## 2.1 Kuka omistaa datan ja tiedon?

Puhuttaessa teollisesta internetistä ja sen hyödyntämisestä datasta herää usein kysymys siitä, kuka on tiedon omistaja ja kuka sitä hallitsee. Lähtökohtaisesti tietoa ja dataa ei omista kukaan lainsäädännön tarkoittamassa merkityksessä. Tietoa ja dataa kuitenkin hallitsee se, joka omistaa palvelun tai palvelun, johon data tai tieto on tallennettuna. Yleensä myös laitteen tai palvelun omistajalla on kyky estää ulkopuolisten pääsy dataan estämällä pääsy laitteeseen. Voidaan katsoa, että jokaisella toimijalla on oma intressinsä hallita laitteissa ja palveluissa syntyvää tietoa ja dataa koko sen elinkaaren ajan. Näitä toimijoita ovat laitteen tai palvelun toimittaja, ohjelmiston valmistaja sekä laitteen tai palvelun omistaja. (Collin ym. 2015, 16.)

Tiedon ja datan omistajuutta voidaan lähestyä myös immateriaalioikeuksien näkökulmasta, vaikka silloinkaan kyse ei varsinaisesti ole omistajuudesta. Patenttilain 1§:n mukaan keksijä voi saada hakemuksesta patentin keksintöön ja siten yksinoikeuden sen ammattimaiseen hyödyntämiseen. Keksinnöksi ei kuitenkaan patenttilain mukaan katsota esimerkiksi suunnitelmaa, sääntöä tai menetelmää, älyllistä toimintaa, peliä tai liiketoimintaa varten taikka tietokoneohjelmaa eikä tietojen esittämistä. Yleisesti immateriaalioikeudet ovat sovittavissa, mutta pakottavaa lainsäädäntöä on kuitenkin olemassa paljon. Esimerkiksi edellä mainittu patenttilaki on pakottavaa lainsäädäntöä. (Sama.)

Immateriaalioikeudet voidaan jakaa tekijänoikeuteen ja teollisoikeuksiin. Molemmat antavat yksinoikeuden määrätä siitä, miten oikeuksia hyödynnetään liiketoiminnassa. Nämä oikeudet ovat ajallisesti rajattuja ja siksi luovat vahvaa omistajuutta, koska niiden avulla voidaan estää datan käyttö muilta. Immateriaalioikeuksia voi kuitenkin syntyä vasta siinä vaiheessa, kun tietoa ja dataa käytetään esimerkiksi osana uusia tuotteita ja palveluita. Silloin kun tietoa tai dataa syntyy suuria määriä, kyseeseen voi tulla tekijänoikeuslain 49 §:n tarkoittama luettelo- ja tietokantasuoja. Tämä ei kuitenkaan suojaa yksittäistä tietoa tai tietokannan epäolennaista osaa, vaan tietokokonaisuutta ja sen sisältämää dataa. (Sama.)

Tiedon omistajuuteen liittyy myös henkilötietojen tietosuoja. Rekisterinpitäjä eli se toimija, joka hallitsee henkilöä koskevaa tietoa, on velvollinen huomioimaan toimissaan tietosuojan lain edellyttämällä tavalla. Raportin mukaan tulevaisuudessa Suomessa voisi olla hyödyllistä säätää laki, jossa säädetään tiedon ja datan omistajuudesta. Joissain maissa tämän suuntaista sääntelyä on jo ole-

massa. Esimerkiksi Kiinassa ja Venäjällä on ryhdytty sääntelemään datapalvelimien sijaintiin liittyviä asioita rajoittamalla datan alueellista käytettävyyttä. Euroopan tietosuoja-asetus sisältää myös rajoituksia siirtää tietoja kolmansiin maihin ja on siten askel kohti datan omistajuuden sääntelyä. (Sama, 7.)

Tiedon omistajuutta voidaan tarkastella toisaalta myös sopimusten näkökulmasta. Sopimusvapauden puitteissa voidaan sopia siitä, kenelle data kuuluu ja millaisia käyttöoikeuksia milläkin taholla dataan on. Sopimuksella ei kuitenkaan ole mahdollista sitoa kolmatta osapuolta. Raportin mukaan datan luotettavuus tulee tulevaisuudessa entistä merkittävämmäksi elementiksi. Tämä muokkaa sopimuskäytäntöjä, koska tietoa ja dataa siirtyy eri rajapintojen kautta eri toimijoiden kesken ja pitkissäkin siirtoketjuissa vahingonkorvausoikeudellinen kausaliteetti tulee pystyä sopimusoikeudellisesti määrittelemään. On kuitenkin otettava huomioon, että joka puolella maailmaa ei välttämättä ole mahdollisuutta luoda tällaisia suoria ja epäsuoria estämiskeinoja, eli paikallista oikeuslaitosta ei välttämättä voida käyttää siihen, että pakotetaan datan käyttäjät lopettamaan sen käyttö. Näin ollen sopimukset määrittelevät tulevaisuudessa sen, miten tiedon ja datan omistajuus määräytyy älykkäissä laite- ja palvelukokonaisuuksissa. (Sama, 17.)

Myös Jaakko Lindgren on asianajotoimisto Castren ja Snellmanin blogissa kirjoittanut teollisesta internetistä ja datan omistajuudesta. Hän toteaa, että teollinen internet edellyttäne laajempaa lain-säädäntökeskustelua erityisesti siitä, miten tietoja voidaan käyttää kaupallisesti. Esiin tulevat haasteet vaativat uudenlaista ajattelua sekä uudenlaisia sopimuksia. (Lindgren 2015.)

## **2.2 Teollinen internet ja henkilötiedot**

Teollisen internetin myötä laitteet tulevat entistä intiimimmäksi osaksi jokaisen arkea esimerkiksi älykellojen, älypuhelimien ja älyimplanttien myötä. Näiden laitteiden tai internetin käyttäjä jättää tietoverkossa liikkueensa itsestään niin sanotun datavanan (data trail). Mitä enemmän laitteita kytetään yhteen internetin välityksellä, sitä leveämmäksi tämä datavana kasvaa. Kertyvä data voi olla, joko anonymiä dataa tai personoituja tietoja. Anonymilla datalla tarkoitetaan tietoja, joita ei pystytä liittämään tiettyyn henkilöön. Personoiduilla tiedoilla taas tarkoitetaan henkilötietoja. (Oesch, Eloranta ja Heino 2017, 132.)

Euroopan tietosuoja-asetuksen mukaan henkilötietotoa ovat kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvä tieto. Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurisen tai sosiaalisen tekijän perusteella. Näin ollen myös tässä opinnäytetyössä käsiteltävänä olevia paikka- ja paikannustietoja voidaan pitää tietosuoja-asetuksen tarkoittamana henkilötietona, jos siitä voidaan tunnistaa luonnollinen henkilö. (Euroopan tietosuoja-asetus, EPNAs (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilö-tietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 4 art. 1 kohta.)

Kuten Ahti Saarenpää on artikkelissaan todennut henkilötietojen suojaa, yksityisyyttä sekä tietosuojalainsäädännön merkitystä arvioitaessa joudutaan ottamaan huomioon myös julkisuusperiaatteen merkitys yhteiskunnassa. Julkisuusperiaatteen mukaan julkisena tarjolla olevien henkilötietojen käsittelyn avulla luodaan erilaisia kuvia ihmisistä sekä heidän identiteetistään sekä yksityisyydestään. Rajoitettaessa henkilötietojen käsittelyä syntyy näin ollen jännitettä henkilötietojen suojan ja julkisuuden välille. (Saarenpää 2016, 329.)

## **2.3 Teollinen internet ja tietoturva**

Tietoturva nousee usein huolenaiheeksi puhuttaessa teollisesta internetistä. Sitä on pidetty useissa kyselyissä jopa teollisen internetin pahimpana esteenä. Collinin mukaan uhkaavuutta lisää usein yritysten ylimmän johdon tietämättömyys tietoturvasta, minkä seurauksena tietoturvasta huolehtimiseen ei varata riittävästi resursseja. (Collin & Saarelainen, 242-245.)

Liikenne- ja viestintävaliokunnan mukaan teollisen internetin keskeinen ongelma on, että laitteiden valmistajien ja niiden käyttäjien tietoisuus muun muassa tietoturvavaatimuksista ei ole riittävällä tasolla. Laitteita voidaan käyttää hyödyksi erilaisissa laittomissa palvelunestohyökkäyksissä ja tämä voi muodostaa uuden tietoturvauhan, mikäli asiaan ei kiinnitetä erityistä huomiota. Erityisesti tietoisuuden lisäämiseen sekä laitteiden standardien kehittämiseen tulee panostaa verkkojen turvallisuuden varmistamiseksi. (LiVL 6/2017 vp— U 19/2017 vp, 6.)

Haasteellisuudestaan huolimatta henkilötietolain (HeTiL, 523/1999) mukaan henkilötiedot on suojattava asianmukaisesti niiden luvaton käsittelyä vastaan (HeTiL, 32§) ja Ahti Saarenpää on artikkelissaan maininnut, että tietoturvallisuus näyttelee henkilötietojen suojan sääntelyssä välttämättä keskeistä osaa. Henkilötietolain tietoturvasäännös on kuitenkin suhteellisuusperiaatteen ilmentymä, eikä täsmällistä tietoturvasoa ole pystytty laissakaan määrittelemään. (Saarenpää 2016, 347.)

Perustuslaki (731/1999) takaa jokaiselle oikeuden elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen (PL 7§). Tämän on toteuduttava myös digitaalisessa ympäristössä. Tulevaisuudessa uhkien tunnistamisesta, riskien hallinnasta ja teknisen tietoturvallisuuden kehittämistä on huolehdittava entistä paremmin. Kyberrikollisten ja muiden toimijoiden aiheuttamat uhat ovat kasvussa ja niihin on varauduttava ennakoivasti. (Valtionvarainministeriö 2017, 21.)

Turvallisuus muuttuu ja kehittyy jatkuvasti, samoin kuin erilaiset uhat ja käsityksemme turvallisuudesta. Keskiössä on kuitenkin aina ihminen. Yhteiskuntaa digitalisoitaessa ihmisten ja ihmisten luottamuksen vahvistamisen tulee olla ensisijalla ja turvallisuuskulttuurin luomisen perustana. Näin toimiessa yhteiskunta ja yritykset pystyvät hyödyntämään kehityksen positiiviset puolet. (Valtionvarainministeriö 2017, 99.)

Jäljempänä tarkemmin käsiteltävä EU:n tietosuoja-asetus parantaa merkittävästi kansalaisten oikeuksia digitalisoituvassa yhteiskunnassa ja samalla asettaa lisävelvoitteita rekisterinpitäjille ja henkilötietojen käsittelijöille. Osa velvoitteista liittyy tietoturvallisuuteen. Tulevaisuudessa on pystyttävä mallintamaan, kuvaamaan ja luokittelemaan kaikki tieto oikein, jota kehittyneet keinoälyjärjestelmät käsittelevät (Valtionvarainministeriö 2017, 105).

## **2.4 Teollinen internet ja lainsäädäntö**

Kuten luvun 2.1 lopussa tuli ilmi, teollinen internet vaatii uudenlaista ajattelua ja luultavasti myös uudenlaisia säädöksiä. Tätä näkemystä puoltaa myös liikenne- ja viestintävaliokunnan lausunto. Kyseessä on Liikenne- ja viestintävaliokuntaan saapunut kirjelmä, johon pyydetään lausuntoa. Kirjelmässä on ehdotettu komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi



yksityiselämän ja henkilötietojen suojaamisesta sähköisessä viestinnässä ja sähköisen viestinnän tietosuojadirektiivin kumoamista. (LiVL 6/2017 vp – U 19/2017 vp, 1.)

Valiokunnan lausunnon mukaan olisi syytä pohtia, onko teollisen internetin osalta syytä EU-tasolla erilaisin toimenpitein ottaa huomioon verkkojen turvallisuus ja yksityisyyden suojaa koskevat vaatimukset. On mahdollista, että osa laitteiden välisestä tiedonsiirrosta sisältää henkilötietoja, jolloin yleinen tietosuoja-asetus tulee sovellettavaksi. Jos henkilötietoja ei kuitenkaan siirry, tulee monissa tapauksissa sovellettavaksi sähköisen viestinnän tietosuoja-asetus. (LiVL 6/2017 vp— U 19/2017 vp, 7)

Tulevaisuudessa verkottuneiden laitteiden välillä siirrettävän tiedon taloudellinen arvo kasvaa ja sen vuoksi olisi tarpeen ratkaista periaatteet, joilla tietoa voidaan hyödyntää. Tärkeää on, että tietoturvaan ja yksityisyyteen liittyvät ongelmat pyritään ratkaisemaan sääntelyllä, mutta samaan aikaan vältetään alan innovaatioiden ja palvelukehityksen tarpeeton rajoittaminen. (Sama.)

Valiokunta on lausunnossaan korostanut, että sääntelyn on oltava riittävän selkeää, jotta kaikilla toimijoilla on selvää, miten uudessa toimintaympäristössä tulee toimia tietoturvan ja yksityisyyden suojan huomioon ottamiseksi, miten esineiden internetiä ja laitteiden hyödyntämistä voidaan kehittää ja millä perusteilla esineiden ja laitteiden välillä siirrettäviä tietoja voidaan käsitellä. (Sama, 8.)

### 3 YKSITYISYYS JA HENKILÖTIETOJEN SUOJA

Yksityiselämän ja henkilötietojen suoja on merkittävä osa perus- ja ihmisoikeuksia. Euroopan ihmisoikeussopimuksen (EIS) mukaan, jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta (EIS 8 artikla 1. kohta). Vastaava kohta löytyy myös kansalaisoikeuksia ja poliittisia oikeuksia koskevasta kansainvälisestä sopimuksesta (KP-sopimus), jonka 17 artiklan mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. (Yhdistyneiden kansakuntien peruskirja, SoppS 1/1956. 17 artikla.) Henkilötietojen suoja ja yksityiselämän suoja on turvattu myös Euroopan perusoikeuskirjassa sekä Suomen perustuslaissa.

Yksityisyys voidaan tietosuojan kannalta määritellä oikeudeksi päättää itseään henkilökohtaisesti koskevien tietojen käsittelemisestä. Perinteisesti yksityisyyttä turvaavan tietosuojan keskiössä on ollut muiden hallussa olevien arkaluonteisten tietojen paljastamisen rajoittaminen. Teknologian, erityisesti automaattisen tietojenkäsittelyn, kehitys on korostanut vaaroja, joita jo pelkkä tietojen kerääminen ja tallettaminen aiheuttaa yksityisyyden suojalle. (Tuori & Kotkas 2016, 724.)

Yksityiselämän käsite voidaan ymmärtää yleiskäsitteeksi. Yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä (HE 309/1993 vp). Lindroos-Hovinheimo kirjoittaa artikkelissaan, että oikeus yksityisyyteen on ymmärretty yhdeksi keskeisimmistä ihmisoikeuksista siksi, että siihen sisältyy jokaisen vapaus elää sekä muokata olemustaan ja identiteettiään tahtomallaan tavalla. (Lindroos-Hovinheimo 2018, 7.)

Yksityiselämän suojaa voidaan rajoittaa vain joissain poikkeuksellisissa tilanteissa. Ihmisoikeussopimuksissa on mainittu rajoittamisen edellytykset. Eduskunnan perustuslakivaliokunnan mietinnössä 25/1994 on katsottu perusoikeuksien rajoittamisen olevan mahdollista, kun rajoitukset ovat laissa säädettyjä, täsmällisiä ja tarkkarajaisia, hyväksyttäviä ja oikeassa suhteessa hyväksyttävään rajoitustarkoitukseen. Rajoitukset eivät saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa. (PeVM 25/1994, 5.)

Yksityisyys nähdään usein dynaamisena kokonaisuutena, johon kuuluu useita ulottuvuuksia. Saarenpää on maininnut yksityisyyden ulottuvuuksiksi 11 erilaista asiakokonaisuutta; fyysisen yksityisyyden, alueellisen yksityisyyden, sosiaalisen yksityisyyden, mediayksityisyyden, anonymiteetin, yksityisyyden henkilötietojen käsittelyssä, tiedollisen omistusoikeuden, oikeuden tulla arvioiduksi oikeassa valossa, potilasyksityisyyden, työelämän yksityisyyden sekä viestintäyksityisyyden. (Saarenpää n.d.). Keskeisin näistä on tämän opinnäytetyön kannalta työelämän yksityisyys.

Yksityisyyden taso riippuu kuitenkin paljon siitä, kuinka paljon ja mitä tietoa yhteiskunta kulloinkin tarvitsee. Korjan mukaan keskeistä on, minkälaisessa roolissa osapuolet esiintyvät ja mikä on alistumisvelvollisuus asemansa vuoksi, sillä jonka yksityisyyteen halutaan puuttua. Yksityisyys on siis myös subjektiivinen kokemus ja riippuu aina asiayhteydestä. (Korja 2016, 109-110.) Esimerkkinä subjektiivisesta kokemuksesta voidaan käyttää eduskunnan oikeusasiamiehen ratkaisua, joka koski valokuvaamista Kelan toimistossa. Kantelija on tapauksessa katsonut muun muassa, että Kela ei suojaa asiakkaidensa yksityisyyttä riittävästi koska toimiston aulassa odottavat voivat kuulla kaikki asiakastapahtuman keskustelut. Kyseessä olevan toimiston asiakaskysely on myöskin osoittanut, että asiakkaat kokevat palvelupisteiden erottamisen pelkillä sermeillä yksityisyyttä vaarantavana tekijänä. Kuitenkin esimerkiksi kantelut, joissa asiakkaat epäilisivät salassa pidettävien tietojen kuulumista muille asiakkaille, ovat olleet harvinaisia. (Eduskunnan oikeusasiamiehen ratkaisu. (EOA dnro 1140/4/11.)

Yhteiskunnassamme tiedosta on tullut liiketoiminnan väline eikä tieto ole enää henkilön itsensä hallinnassa. Henkilötiedot ovat luoneet uudenlaisen markkinan jota yritykset pyrkivät hyödyntämään. Jokainen on törmännyt näennäisesti ilmaisiin palveluihin internetissä, mutta harva tulee ajatelleeksi, että nämä palvelut eivät oikeasti ole ilmaisia vaan tuottavat rahaa keräämällä henkilötietoja, kun palvelun tarjoajat myyvät tiedot markkinoijille, jotta viestintää pystyttäisiin kohdentamaan tehokkaammin. (Heino 2016, 15.) Useat käyttäjät ovat tähän asti olleet tietämättömiä tai suhtautuneet henkilötietojensa kaupallistamiseen huolettomasti. Ihmisten yksityisyyteen liittyviä asenteita on viime aikoina kuitenkin tutkittu useissa tutkimuksissa. Tutkimuksien mukaan ihmiset suhtautuvat yksityisyyteensä hyvin eri tavoin; osa huolettomasti ja osalla taas on todella tiukka asenne omia tietojaan ja yksityisyyttään kohtaan. Tulevaisuudessa ihmisten tietous ja asenteet yksityisyydestään todennäköisesti tiukentuvat. Tähän vaikuttaa osaltaan myös Euroopan tietosuojasetus, joka rajoittaa yritysten henkilötietojen keräämistä. (Heino 2016, 16.)

Yksityisyys on henkilötietojen suojaan keskeisesti liittyvä käsite. Henkilötietojen suoja on tietosuojalainsäädännön avulla toteutettavaa perusoikeuksien suoja. Kyseessä on ennen kaikkea yksilön suoja, ei niinkään tietojen suoja. (HE 125/2003 vp, 9). Henkilötietojen suojaa käytetään usein kuitenkin virheellisesti synonyymina tietosuojan kanssa, vaikka ne eroavat toisistaan. (Korja 2016, 115.) Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista henkilöön yhdistettävissä olevien tietojen käsittelyssä ja näin ollen henkilötiedot on suojattava oikeudettomalta tai jollakin tavoin henkilöä vahingoittavalta käytöltä. Paul de Hertin ja Serge Gutwirthin (2009) mukaan tietosuoja on luonteeltaan eräänlainen henkilötietojen käsittelyyn liittyvä yleiskäsite. (Korja 2016.)

## 4 HENKILÖTIETOJEN KÄSITTELY

Henkilötietolaki on säädetty toteuttamaan yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä. Henkilötietolaki on yleislaki, minkä takia mahdollisia muissa laissa olevia henkilötietojen käsittelyä koskevia erityissäännöksiä sovelletaan ensisijaisesti.

Tämän opinnäytetyön kirjoittamishetkellä henkilötietojen käsittelyä koskeva lainsäädäntö on uudistumassa 25.5.2018 sovellettavaksi tulevan Euroopan tietoturva-asetuksen johdosta. Hallitus on jättänyt eduskunnalle esityksen EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi ja esityksessä ehdotetaan säädettäväksi tietosuojalaki. Samalla ehdotetaan henkilötietolain sekä lain tietosuojalautakunnasta ja tietosuojavaltuutetusta kumoamista. (HE 9/2018 vp.)

### 4.1 Euroopan tietosuoja-asetus

Tietosuoja-asetus on annettu henkilötietojen suojaa koskevan Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan 1 kohdan nojalla. (HE 9/2018 vp.) Tietosuoja-asetus astui voimaan 24.5.2016 ja sitä sovelletaan kahden vuoden siirtymäajan jälkeen 25.5.2018 alkaen, jolloin henkilötietojen käsittelyn on oltava tietosuoja-asetuksen mukaista. (Euroopan tietosuoja-asetus 99 art.)

Tietosuoja-asetuksen soveltamisalaan kuuluu kaikki henkilötietojen käsittely, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittely muussa kuin automaattisessa muodossa, joka muodostaa rekisterin osan tai joiden tarkoitus on muodostaa rekisterin osa. (Euroopan tietosuoja-asetus 2.1 art.) Asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei. (Euroopan tietosuoja-asetus 3.1 art.) Soveltamisalaa rajaavat sen aineellista ja alueellista soveltamisalaa koskevat säännökset. Asetusta sovelletaan asetuksessa määritellyissä tilanteissa myös EU:n ulkopuolelle sijoittuneisiin organisaatioihin. Soveltamisalaan kuuluvat sekä yksityinen että julkinen sektori. (Oikeusministeriö 2017, 9.)

Asetuksen tarkoituksena on ollut ajantasaistaa tietosuojaa koskevaa sääntelyä, jotta voidaan vastata teknologian kehitykseen ja henkilötietojen suojaa koskeviin haasteisiin. Asetus yhdenmukaistaa myös sääntelyä jäsenvaltioissa ja tukee näin myös digitaalitalouden kehitystä sisämarkkinoilla. (HE 9/2018 vp, 4). Tietosuoja-asetuksella kumotaan vuonna 1995 annettu henkilötietodirektiivi (HE 9/2018vp, 27).

Digitalisoituvassa maailmassa tieto- ja kyberturvallisuuden merkitys on kasvanut merkittävästi. Digitalisaatio on luonut uusia tapoja kerätä, käsitellä ja hyödyntää tietoa. Näiden uusien tapojen rinnalla myös tietoverkkorikollisten, terroristien- ja ääriyhtymien sekä valtiollisten tiedusteluorganisaatioiden muodostamat uhat ovat lisääntyneet. (EU:n tietosuojan kokonaisuudistus 2016, 7.) Aiemmin EU on vaikuttanut tieto- ja kyberturvallisuusturvallisuuden kehittämiseen laatimalla kyberturvallisuusstrategian sekä verkko- ja tietoturvadirektiivin (NIS). Tietosuoja-asetus täydentää tätä kehitystä siten, että kaikki keskeiset velvoitteet on päivitetty vastaamaan ympäristön ja teknologiakehityksen edellyttämiä vaatimuksia. (EU:n tietosuojan kokonaisuudistus 2016, 7.)

Tietosuoja-asetus lisää henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä tarjoaa rekisteröidylle entistä paremmat oikeudet valvoa henkilötietojensa käsittelyä. Samalla asetus asettaa rekisterinpitäjälle uusia velvollisuuksia. Asetuksen noudattamista tuetaan aiempaa ankarimmilla sanktioilla, mikäli henkilötietoja käsitellään asetuksen vastaisesti. (Oikeusministeriö 2017, 9.)

#### **4.1.1 Merkittävimmät muutokset**

Euroopan tietosuoja-asetuksessa on paljon aiempaa henkilötietolakia vastaavaa sääntelyä. Esimerkiksi asetuksen ydinkäsitteet, käsittelyperusteet sekä tietojen siirtoa EU- tai ETA-alueen ulkopuolelle koskevat säännökset ovat pääpiirteissään samat kuin henkilötietolaissa. Tietosuoja-asetukseen on kuitenkin myös uusia elementtejä. Näitä ovat sisäänrakennettu tietosuoja (privacy by design) ja oletusarvoinen tietosuoja (privacy by default). Ensimmäinen tarkoittaa, sitä että tietosuoja tulisi ottaa huomioon jo tuotteita ja palveluita suunniteltaessa niiden koko elinkaaren ajan. Oletusarvoinen tietosuoja sen sijaan tarkoittaa, että yksityisyydensuojaa edistävät oletusarvot (asetukset) ovat automaattisesti käytössä esimerkiksi sosiaalisessa mediassa ja mobiilisovelluksissa. (Tietosuojavaltuutetun toimisto 2016.)

Näiden lisäksi uutta asetuksessa on rekisterinpitäjälle asetettu osoitusvelvollisuus, ilmoitukset tietoturvaloukkauksista, mahdollinen velvollisuus nimittää tietosuojavaltuutettu sekä sanktiot. Lisäksi rekisteröidyn oikeudet ovat osittain asetuksen myötä laajentuneet. Rekisteröidyn oikeuksia käsitelään jäljempänä tässä opinnäytetyössä.

Asetus muuttaa myös rekisterinpitäjän ja henkilötietojen käsittelijän välistä vastuun jakautumista. Henkilötietolain mukaan rekisterinpitäjällä on ollut vastuu käsittelyn lainmukaisuudesta ja käsittelijän vastuu on syntynyt vain sopimuksen kautta. Euroopan tietosuoja-asetuksen mukaan rekisterinpitäjällä on päävastuu käsittelyn lainmukaisuudesta, mutta käsittelijälle on asetettu myös velvoitteita kuten käsittelytoimien dokumentointivelvollisuus. Asetuksen mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on kuvattava vastuut kirjallisessa sopimuksessa. Rekisteröity voi myös kohdistaa korvausvaatimuksensa asetuksen mukaan suoraan käsittelijään. (Euroopan tietosuoja-asetus luku 5.)

#### **4.1.2 Henkilötietojen käsittelyä koskevat periaatteet tietosuoja-asetuksessa**

Euroopan tietosuoja-asetuksessa henkilötietojen käsittelylle on asetettu tiettyjä periaatteita, joita rekisterinpitäjän on noudatettava. Periaatteet ovat:

1. Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
2. Käyttötarkoitussidonnaisuus
3. Tietojen minimointi
4. Täsmällisyys
5. Säilytyksen rajoittaminen
6. Tietojen eheys ja luottamuksellisuus
7. Osoitusvelvollisuus

(Euroopan tietosuoja-asetus 5 art.).

Asetuksen mukaan rekisterinpitäjä on vastuussa siitä, että henkilötietoja ei käsitellä ilman asianmukaista oikeusperustaa. Tämä tarkoittaa, että asetuksessa mainituista lainmukaisuuden edellytyksistä vähintään yhden on täyttyvä, jotta käsittely olisi lainmukaista. Näitä edellytyksiä ovat

rekisteröidyn vapaaehtoinen suostumus, sellaisen sopimuksen täytäntöön paneminen, jossa rekisteröity on osapuolena, rekisterinpitäjän lakisääteinen velvoite, rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen ja rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen. Rekisterinpitäjän on asetuksen mukaan ennakkoon määriteltävä ne tarkoitukset, joihin tietoja käsitellään ja varmistuttava siitä, että tietoja ei käsitellä muihin kuin näihin tarkoituksiin. (Euroopan tietosuoja-asetus 6 art.)

Mikäli henkilötietojen käsittely perustuu rekisteröidyn suostumukseen, on suostumuksen oltava vapaaehtoinen, yksilöity ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla suostumusta ilmaisevan toimen. Aktiivinen suostumus tarkoittaa suostumusta, joka ei sisällä esitetyistä valintoja ja on selkeästi erillään muista ehdoista. Suostumus ei myöskään saa olla palvelun edellytys, ellei palvelu vaadi henkilötietojen käsittelyä. Suostumuksen on oltava peruutettavissa, milloin tahansa ja rekisteröidylle on annettava selkeät ohjeet suostumuksen peruuttamiseen. Rekisterinpitäjällä on osoitusvelvollisuus suostumusten osalta eli jokainen suostumus on dokumentoitava.

(Euroopan tietosuoja-asetus 7 art.)

Tietosuoja-asetuksen asettamien velvoitteiden laiminlyönnistä tai rikkomisesta voi rekisterinpitäjälle tai henkilötietojen käsittelijälle aiheutua hallinnollisia sakkoja, jotka ovat 2% (10MEUR) tai 4% (MEUR) globaalista liikevaihdosta. Sakkojen määrään vaikuttavat muun muassa rikkomuksen luonne, vakavuus, kesto, rekisteröidylle aiheutuneen vahingon suuruus, tahallisuus, yhteistyön aste valvontaviranomaisen kanssa sekä tapa, jolla asia tuli valvontaviranomaisen tietoon. (Euroopan tietosuoja-asetus 83 art.)

Rekisterinpitäjä on asetuksen mukaan vastuussa myös siitä, että käsiteltävät henkilötiedot ovat asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Tietojen on oltava siis täsmällisiä ja tarvittaessa päivitettävissä. Rekisterinpitäjän on poistettava tai oikaistava epätarkat ja virheelliset tiedot viipymättä. (Euroopan tietosuoja-asetus 5 art.)

Rekisterinpitäjän on säilytettävä tietoja muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin se on tarpeen tietojen käsittelyn tarkoituksen toteutumista varten. Kun tämä tarve loppuu, on rekisterinpitäjän huolehdittava siitä, että tiedot poistetaan tai arkistoidaan. (Euroopan tietosuoja-asetus 5 art.)



Rekisterinpitäjän on käsiteltävä henkilötietoja tavalla, jolla varmistetaan niiden asianmukainen turvallisuus mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia. (Euroopan tietosuoja-asetus 5 art.)

#### **4.1.3 Rekisteröidyn oikeudet**

Rekisteröidyllä on tietosuoja-asetuksen mukaan oikeus saada pääsy tietoihin. Tämä tarkoittaa, että rekisterinpitäjän on rekisteröidyn pyynnöstä ilmoitettava, käsitelläänkö tätä koskevia henkilötietoja vai ei. Lisäksi rekisteröidyllä on oikeus saada jäljennös häntä koskevista henkilötiedoista. Rekisteröidyllä on oikeus saada tieto käsittelyn tarkoituksista, käsiteltävinä olevista henkilö-tietoryhmistä, vastaanottajista sekä mahdollisuuksien mukaan henkilötietojen suunniteltu säilytysaika. Rekisteröidylle on myös ilmoitettava oikeudesta tehdä valitus valvontaviranomaisella, tieto automaattisen päätöksenteon käyttämisestä tai profiloinnista sekä mikäli henkilötietoja siirretään kolanteen maa-han, tieto tietosuojan riittävyyden huomioimisesta. (Euroopan tietosuoja-asetus, 15 art.) Tämä vas-taa aiempaa henkilötietolain 26 §:ssä säädettyä rekisteröidyn tarkastusoikeutta.

Rekisteröidyllä on tietosuoja-asetuksen mukaan oikeus tietojen oikaisemiseen. Tämä tarkoittaa, että rekisterinpitäjän on viipymättä oikaistava virheelliset henkilötiedot. (Euroopan tietosuoja-ase-tus 16 art.) Mikäli henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin, rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, rekisteröity vastustaa käsittelyä eikä käsittelylle ole olemassa perusteltua syytä tai henkilötietoja on käsitelty lainvastaisesti, on rekisterinpitäjällä velvollisuus poistaa tiedot ilman aiheetonta viiväs-tystä. Tätä kutsutaan tietosuoja-asetuksessa oikeudeksi tulla unohdetuksi. Tietoja ei kuitenkaan ole mahdollista poistaa lakisääteisen tehtävän suorittamiseen liittyvän käsittelyn yhteydessä. (Eu-roopan tietosuoja-asetus 17 art.)

Mikäli henkilötietojen käsittely perustuu suostumukseen, on rekisteröidyllä oikeus saada häntä kos-kevat henkilötiedot siirretyksi järjestelmästä toiseen yleisesti käytössä olevassa siirtomuodossa. (Euroopan tietosuoja-asetus 20 art.) Tällaista oikeutta ei henkilötietolaissa mainittu, joten kyseessä on uusi rekisteröidyn oikeus.

Tietyissä tilanteissa rekisteröidyllä on oikeus vastustaa häntä koskevien henkilötietojen käsittelyä. Tällaisiksi tilanteiksi on mainittu asetuksessa tilanne, jossa rekisteröity henkilökohtaiseen erityiseen tilanteeseen liittyvällä perusteella vastustaa henkilötietojensa käsittelyä, joka perustuu asetuksen 6 artiklan 1 kohdan e tai f alakohtaan. Rekisteröidyllä on lisäksi oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä, mikäli henkilötietoja käsitellään suoramarkkinointia varten. (Euroopan tietosuoja-asetus 21 art.)

Näiden edellä mainittujen oikeuksien lisäksi rekisteröidylle on asetuksessa säädetty oikeus saada ilmoitus tietoturvaloukkauksista. Tämä tarkoittaa, että rekisterinpitäjän on ilmoitettava henkilökohtaisesti tietoturvaloukkauksista niille rekisteröidylle, joita loukkaus koskee. Velvollisuus astuu voimaan, jos loukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille. (Euroopan tietosuoja-asetus 34 art.)

## **4.2 Tietosuoja laki**

Hallituksen esityksen mukaan uuden tietosuojalain tarkoituksena on täsmentää ja täydentää yleistä tietosuoja-asetusta. Asetuksen luonne poikkeaa direktiivistä siten, että asetusta ei lähtökohtaisesti salli kansallista edes asetuksen mukaista lainsäädäntöä (HE 9/2018 vp, 27). Tästä syystä tietosuoja-asetus on suoraan sovellettavaa lainsäädäntöä, ja asetusta voidaan täsmentää ainoastaan yleisessä tietosuoja-asetuksessa annetun kansallisen liikkumavaran puitteissa. (HE 9/2018vp, 4).

Ennen yleisen tietosuoja-asetuksen ja tietosuojalain voimaantuloa henkilötietojen käsittelyn perusteista on säädetty henkilötietolaissa, joka on tullut voimaan 1.6.1999. Tällä lailla saatettiin henkilötietojen käsittelyä koskeva yleislainsäädäntö vastaamaan yksilöiden suojelusta henkilötietojen käsittelystä ja näiden tietojen vapaasta liikkuvuudesta annettua henkilötietodirektiiviä. (HE 9/2018vp, 6). Henkilötietodirektiivin antamisesta on kuitenkin yli 20 vuotta ja henkilötietojen suojeleminen on teknologian kehittymisen myötä kohdannut uudenlaisia haasteita. Hallituksen esityksessä ehdotetaankin henkilötietolain kumoamista kokonaisuudessaan sekä tietosujalautakunnasta ja tietosujavaltuutetusta annettujen lakien kumoamista. (HE 9/2018 vp, 52.)

Nykyistä henkilötietolakia on kuitenkin pyritty pitämään lähtökohtana uuden tietosuojalain esityksessä ja tavoitteena on, että tietosuojalaki olisi selkeästi yleislaki. (HE 9/2011vp, 52). Tietosuojalakia on tarkoitus soveltaa tietosuoja-asetuksen kanssa rinnakkain ja soveltamisalaltaan tietosuojalain ehdotetaan olevan yleisen tietosuoja-asetuksen 2 artiklan mukainen. Asetusta sekä tietosuojalakia sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn, jotka muodostavat rekisterin tai sen osan. (HE 9/2018 vp, 6.)

Osana tietosuojalainsäädännön kansallista toimeenpanoa Valtioneuvoston kanslia rahoitti yleisen tietosuoja-asetuksen kansallista toimeenpanoa selvittäneen erillishankkeen. Hankkeessa IPR University Cernin, Helsingin yliopiston ja Lapin yliopiston tutkijat kävivät läpi satoja säädöksiä ja arvioivat niiden ja tietosuoja-asetuksen yhteensopivuutta. Henkilötietolaki ei ollut arvioinnin kohteena. Lopputuloksena todettiin, että henkilötietojen käsittelyn perusteet vastasivat hyvin tietosuoja-asetuksen mukaisia henkilötietojen käsittelyn periaatteita. (Valtioneuvosto 2017, 11) Osana tätä hanketta tehtiin myös tietosuoja-asetuksen yritysvaikutuksia koskeva selvitys. Tämän selvityksen mukaan tietosuoja-asetus lisää merkittävästi yritysten hallinnollisia tehtäviä ja aiheuttaa oikeudellista epävarmuutta. (Collin ym. 2017, 2.)

## 5 HENKILÖTIETOJEN KÄSITTELY TYÖSUHTEESSA

Automaattisen tietojenkäsittelyn kehitys sekä käyttö ovat merkinneet henkilötietoja sisältävien rekisterien syntymistä yhä laajemmin myös työelämässä. Tästä syystä henkilöstöhallinnon rekisterit ovat erityisen merkityksellisiä. Työntekijän yksityisyyden suoja on viime vuosina noussut yhdeksi keskeisimmistä keskustelunaiheista työelämässä. (Korja 2015, 99.)

Työelämän yksityisyyden suojaa säädellään lailla yksityisyyden suojasta työelämässä (YksTL). Lain tavoitteena on turvata mahdollisimman hyvä yksityisyyden suoja työnhakijoille, työntekijöille ja virkamiehille. Henkilötietolaki on yleislaki eikä sitä siitä syystä ole voitu pitää työelämän kannalta riittävänä. (HE 75/2000 vp, 10.)

YksTL 3 §:n mukaan työnantajalla on oikeus käsitellä vain työsuhteen kannalta välittömästi tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erikoisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella.

Henkilötietojen käsittelyä voidaan katsoa käytettäväksi myös vallankäytön välineenä. Erilaiset organisaatiot pyrkivät hallitsemaan ihmisiä niin kansalaisina, asiakkaina kuin työntekijöinäkin. Tämä hallinta edellyttää usein ihmisen tunnistamista. Korjan mukaan osana yleisempää yksityisyyden suojan menettämisen tunnetta tämä voi johtaa siihen, että monet myös kokevat vastenmielisyyttä tunnistamiseen. Henkilötietojensuojan näkökulmasta yksityisyyden suurin merkitys työelämässä on, että se tasoittaa työnantajan ja työntekijän välistä tiedollista epätasapainoa (Korja 2016, 83-84.)

EU:n kansallisista tietosuojaviranomaisista koostuva WP29-ryhmä on ottanut kantaa työelämän tietojenkäsittelyyn. Kannanotossaan WP29 esittelee erilaisia skenaarioita, joissa työnantaja voi aiheuttaa korkeaa riskiä työntekijöidensä yksityisyyden suojalle. Kannanotossa on mainittu muun muassa erilaisten ajoneuvojen GPS paikannus. Ajoneuvon paikantamisella on mahdollista saada sijaintitietoa myös sitä kuljettavasta henkilöstä ja näin ollen kyseessä on välillinen paikantaminen. Työnantajan on aina tämän kaltaista teknologiaa käyttäessään arvioitava tietojenkäsittelyn välttämättömyyttä sekä otettava huomioon työntekijöiden läpinäkyvä informointi (WP 2/2017, 19.)

Lausunnossa on tuotu myös esille BYOD (Bring your own device) toimintamalli, jossa työntekijä käyttää pääsääntöisesti omia päätelaitteitaan työnsä tekemiseen. Toimintamallilla on omat hyötynsä ja se saattaa parantaa työntekijän työtyytyväisyyttä lisäämällä työnteon joustavuutta, mutta se mahdollistaa myös yksityisyyttä loukkaavien tietojen keräämisen. Tästä syystä on tärkeää, että työnantaja harkitsee tiettyjen työvälineiden yksityiskäytön kieltämistä, mikäli yksityisten tietojen tallentamisen rajoittaminen ja tarkkailu ei ole mahdollista. (WP 2/2017, 16- 17.)

Markus Pervilä on artikkelissaan kirjoittanut BYOD-mallin ongelmista ja kertoo, työntekijöiden olevan erityisen huolestuneita mobiililaitteiden paikannuspalveluista. Siksi BEYOD- sopimuksissa on hyvä mainita erikseen, ettei työnantaja saa kerätä laitteiden avulla paikannustietoja. (Pervilä, 2013.)

## **5.1 Paikka- ja sijaintitiedot**

Paikkatiedolla tarkoitetaan tietoa, joka on kiinnitetty sijaintiin. Paikkatieto voi olla välitön esimerkiksi koordinaatit, tai välillinen, kuten esimerkiksi osoite joka viittaa paikkaan tai alueeseen. Paikkatietoon liittyy ominaisuustieto, joka kuvaa, mitä sijaintitiedon esittämässä sijainnissa on. (Korpisaari 2018, 22). Laissa paikkatietoinfrastuktuurista (paikkatietolaki, 421/2009) paikkatieto on määritelty tiedoksi, joka sisältää välittämän tai välillisen viittauksen tiettyyn paikkaan tai maantieteelliseen alueeseen (Paikkatietolaki 2§ 1. mom.)

Sijaintitieto ilmaisee kohteen sijainnin esimerkiksi osoitteella tai koordinaateilla. Sijaintitiedon avulla voidaan yhdistää samaan kohteeseen liittyviä tietoja ja sijaintitieto voi saman ihmisen osalta vaihdella useita kertoja vuorokaudessa. (Maanmittauslaitos 2017, 5.)

## **5.2 Työntekijän paikantamisen edellytykset**

Työntekijän paikantaminen on teknistä valvontaa ja sen edellytyksistä säädetään laissa yksityisyyden suojasta työelämässä (YksTL, 2004/759). Tietosuojavaltuutetun mukaan työnantajalla saattaa joissain tilanteissa olla erityinen tarve työntekijän paikantamiseen. Tällaisia tilanteita voivat olla esimerkiksi työntekijöiden turvallisuuden varmistaminen tai resurssien kohdentaminen oikeaan paikkaan. (Tietosuojavaltuutetun toimisto, 2018.) Paikannuksen käyttäminen edellyttää kuitenkin aina

suostumuksen pyytämistä työntekijältä. Suostumuksen edellytyksistä henkilötietojen käsittelyn yhteydessä on säädetty Euroopan tietosuoja-asetuksen 7 artiklassa. Aihetta on käsitelty tarkemmin tämän opinnäytetyön luvussa 4.1.2.

Paikantamispalveluilla saadaan hyvin yksityiskohtaista tietoa henkilön sijainnista ja tämän vuoksi työntekijä voi kokea yksityisyytensä loukatuksi ja vastustaa paikantamista. Työnantajalla on kuitenkin työsuhteessa niin sanottu johto- ja valvontaoikeus (direktio-oikeus) eli työntekijä on sitoutunut tekemään töitä työnantajan johdon ja valvonnan alaisena. Työsopimuslain mukaan työnantaja voi direktio-oikeutensa nojalla määrätä miten, missä ja milloin työ tulee suorittaa (TSL 3:1 §). Paikantamispalveluiden käyttäminen voi olla osa tätä organisointia ja kun työtä tehdään muualla kuin työnantajan tiloissa, voi paikannus olla tarpeellista esimerkiksi työntekijän turvallisuuden takaamiseksi.

Mikäli työnantajan tarkoituksena on paikantaa työntekijöitään paikannusjärjestelmän avulla, tulee paikantamiselle olla etukäteen määritelty asiallinen käsittelyn peruste ja käyttötarkoitus. Tästä on säädetty aiemmin henkilötietolain 6 §:ssä ja nykyisin käsittelyn lainmukaisuudesta säädetään Euroopan tietosuoja-asetuksen 6 artiklassa. Tällaisia asiallisen käsittelyn perusteita voivat olla työntekijöiden turvallisuuden varmistaminen tai resurssien ohjaaminen oikeaan paikkaan. Työntekijällä on kuitenkin edelleen oikeus kieltäytyä paikantamisesta, mutta tällöin voi syntyä tilanne jossa työnantaja voi joutua harkitsemaan työntekijän työsuhteen ehtojen muuttamista tai päättämistä.

### **5.3 Välitön ja välillinen paikantaminen**

Paikantaminen voidaan jakaa välittömään ja välilliseen. Välillinen paikantaminen tarkoittaa, että paikantaminen on järjestetty siten, että paikannetaan esimerkiksi ajoneuvoa tai muita liikkuvia kohteita. Esimerkiksi ajoneuvon paikannustilanteessa, jossa työntekijä voidaan tunnistaa työ- ja ajovuorolistojen avulla tulevat YksTL:n 21 §:n säännökset yhteistoimintamenettelystä sovellettavaksi työnantajan suorittaessa työntekijöihin kohdistuvaa teknistä valvontaa. Erillistä suostumusta paikantamiseen ei tällöin tarvita, mikäli asiallisen käsittelyn periaatteet toteutuvat ja paikantamisen periaatteet on käyty läpi yhteistoimintamenettelyssä. Lisäksi asiasta on tiedotettava työntekijöitä. (Tietosuojavaltuutettu dnro 87/41/2010.)

Välittömässä paikantamisessa paikannus kohdistuu suoraan työntekijään esimerkiksi matkapuhelimen tai muun GPS-paikannuksen avulla. Tietosuojavaltuutetun näkemyksen mukaan välittömään paikantamiseen tulisi aina olla työntekijän suostumus. Tietosuojavaltuutettu on tulkinnessaan viitannut sähköisen tietosuojalain 16-18 §:ien säännöksiin. (Tietosuojavaltuutettu dnro 87/41/2010.)

Mikäli paikannusjärjestelmää on tarkoitus käyttää työajan valvontaan ja seurantaan, tulee tämä määritellä etukäteen paikantamisen käyttötarkoitukseksi ja olla asiallisesti perusteltua, esimerkiksi työtä suoritetaan kokonaan tai enimmäkseen muualla kuin työnantajan tiloissa eikä työajanvalvontaan ei ole käytettävissä muita vähemmän yksityisyyden suojaan puuttuvia keinoja. Tällaisen paikantamiseen perustuvan työajan seurantarjestelmän tulee olla mahdollisimman selkeä ja määriteltä sekä mahdollisesti erillinen järjestelmä. Työntekijöillä tulee olla selkeät ohjeet siitä, kuinka työajan seurantarjestelmää käytetään ja mitä henkilötietoja se kerää työntekijöistä työajanseuranta varten. (Alapuranen 2016, 142.)

Työnantajan on huolehdittava siitä, että työntekijällä on mahdollisuus kytkeä paikannus pois päältä erityisesti silloin kun päätelaitetta voi luvallisesti käyttää myös työajan ulkopuolella. Direktio-oikeus ei ulotu työajan ulkopuolelle ja työnantajan on myös huolehdittava, ettei tahattomasti päälle jäänyt paikannus tuota oikeudettomasti tietoa työnantajalle. Työnantajan on lisäksi varmistettava, että paikannuksen tarvetta on arvioitu työtehtäväkohtaisesti ja työntekijät, joihin se kohdistuu ovat siitä tietoisia. (Sama.)

Luonnolliseen henkilöön yhdistettäviä sijaintitietoja saa käsitellä lisäarvopalvelun hyödyntämiseksi, vain jos henkilö on antanut siihen suostumuksensa. Laissa sähköisen viestinnän palveluista lisäarvopalvelulla tarkoitetaan palvelua, joka perustuu välitystietojen tai sijaintitietojen käsittelyyn muuta kuin viestin välittämistä varten. Sijaintitietoja saa käsitellä vain käsittelyn tarkoituksen vaatimassa laajuudessa eikä käsittelyllä saa rajoittaa yksityisyyden suojaa enempää kuin on välttämätöntä. Käsittelyn jälkeen sijaintitiedot on hävitettävä tai anonymisoitava. (TYK 160.3 §.)

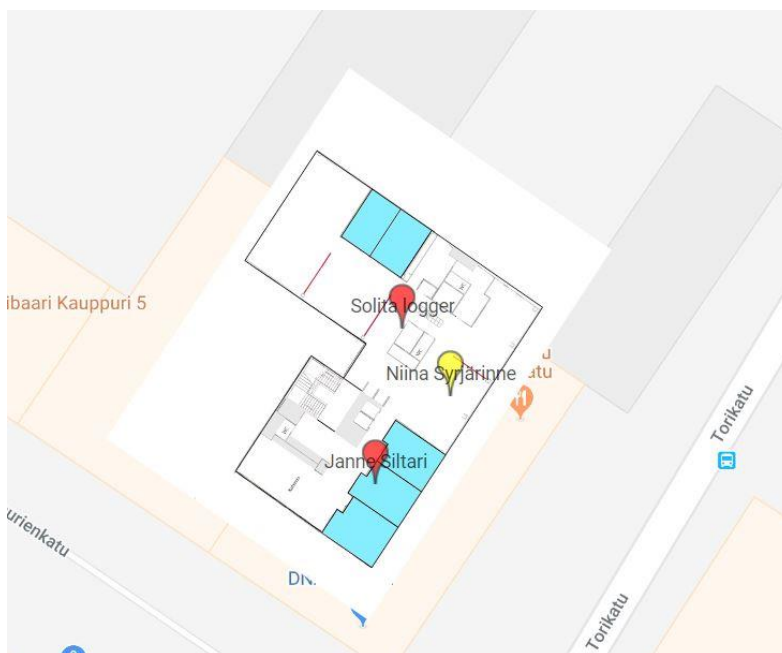
Paikannettavalla henkilöllä on myös oikeus paikantamista koskeviin tietoihin. Sähköisen viestinnän palveluista annetun lain 161 §:n mukaan paikannettavan saatavilla on oltava helposti ja jatkuvasti tietoa käsiteltävien sijaintitietojen tarkkuudesta, käsittelyn täsmällisestä tarkoituksesta ja kestosta sekä siitä, voidaanko sijaintitiedot luovuttaa kolmannelle osapuolelle lisäarvopalvelun tarjoamista varten. Lisäksi saman lain 162 §:n mukaan henkilöllä on oikeus saada lisäarvopalvelun tarjoajalta

ja viestinnän välittäjältä näiden hallussa olevat häntä itseään koskevat sijaintitiedot ja välitystiedot, jotka ilmaisevat liittymän tai päätelaitteen sijainnin tietyllä hetkellä.

#### 5.4 Solita sisätilapaikannus Proof of concept (POC)

Solitan Oulun toimistolle luotiin sisätilapaikannuksesta eräänlainen demovaihe (POC eli Proof of Concept). Demovaiheen tarkoituksena oli havainnollistaa ja testata sisätilapaikannuksen toimivuutta toimistoympäristössä. Sisätilapaikannus toteutettiin Bluetoothin avulla toimivien ihmisiin tai esineisiin kiinnitettyjen niin sanottujen Bluetooth majakoiden (beacons) avulla. Bluetooth on radioaaltoihin perustuva lyhyen kantaman langaton tiedonsiirtotekniikka. Bluetoothin avulla toimivat tagit eivät tarvitse toimiakseen erillisiä tukiasemia, vaan matkapuhelimet toimivat niiden tukiasemina. Beaconit lähettävät omaa tunnustaan älypuheliin, joka taas lähettää sitä edelleen taustajärjestelmään. Taustajärjestelmä tunnistaa majakan sijainnin ja lähettää takaisin älypuheliin paikkaan liittyvän vastineen. (Heino 2016, 23.)

Mukana kuljetettavat beaconit annettiin kolmelle työntekijälle. He pystyivät näkemään puhelimeensa asennetun sovelluksen avulla rakennuksen pohjapiirustuksesta reaaliaikaisesti, missä kukin liikkuu (Kuva 1.) Samantapaista ratkaisua olisi mahdollista käyttää myös esimerkiksi tehtaissa laitteiden liikkumisen seuraamiseen.



KUVA 1. Oulun toimiston pohjapiirustus



Sisätilapaikannusmenetelmää käytettiin myös IoT Nordic Week 2018 tapahtumassa, jossa Solita oli mukana (Kuva 2.) Kyseessä on viisipäiväinen tapahtuma, jossa käsitellään ajankohtaisia teemoja kuten IoT, teollinen internet, koneoppiminen, alustat ja ekosysteemit. Tapahtumaa varten luotiin Helsingin kattilahalliin samanlainen demoympäristö kuin Solitan Oulun toimistolla. Pohjapiirustuksen ja Beaconejen avulla pystyttiin seuraamaan messuilla mukana olleiden työntekijöiden liikkeitä.



KUVA 2. Kattilahallin pohjapiirustus

Paikannusdemoa ei käytetty varsinaisesti mitään määriteltyä tarkoitusta varten. Demon tarkoituksena oli toimia esimerkkinä ja testinä, kuinka hyvin ja tarkasti paikannus toimiston sisällä pystytettiin toteuttamaan. Samalla demo herätteli miettimään seurattavien tuntemuksia liittyen yksityisyyteen ja paikantamiseen sekä pohtimaan mahdollisia käyttötilanteita paikannusratkaisuille.

## 5.5 Yhteistoimintamenettely

Työsuhteen aikana kerättävät henkilötiedot tulee käydä läpi työpaikan yhteistoimintamenettelyssä siten, kuin YksTL:n 4 §:n 3 momentissa säädetään. Tämän pykälän mukaan henkilötietojen kerääminen työhön otettaessa ja työsuhteen aikana kuuluu yhteistoimintaneuvotteluista yrityksissä annetussa laissa (yhteistoimintalaki, 334/2007) tarkoitetun yhteistoimintamenettelyn piiriin. Julkisella

sektorilla sovelletaan lakia yhteistoiminnasta valtion virastoissa ja laitoksissa (651/1988) sekä kunnissa lakia työnantajan ja henkilöstön välisestä yhteistoiminnasta (44/2007).

Tietosuojavaltuutettu on antanut 22.12.2010 päätöksen koskien paikantamista työelämässä (dnro 87/41/2010). Päätöksessään tietosuojavaltuutettu toteaa, että työntekijöihin kohdistuvan kamera-valvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät kuuluvat yhteistoiminnasta yrityksissä annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Paikantamista koskeva asia tulee siis käsitellä yhteistoimintamenettelyssä työelämän tietosuojalain 21 §:n mukaisesti ennen kuin teknisin menetelmin toteutettu valvonta voidaan ottaa käyttöön organisaatioissa. Tietosuojavaltuutetun mukaan tämä tarkoittaa seuraavia toimenpiteitä:

- Henkilötietojen keräämisen etukäteismäärittely
- Henkilötietojen asiallinen perustelu paikantamisen kannalta
- Rekisteriselosteen laadinta ennen henkilötietojen keräämistä
- Määrittely, kenellä organisaatiossa on oikeus käsitellä paikantamisessa kertyviä henkilötietoja
- Henkilötietojen säilyttämisaikojen määrittely asiallisen käsittelyn perusteen ja tarpeellisuusvaatimuksen mukaisesti. (Tietosuojavaltuutettu 87/41/2010.)

Yhteistoimintalain tarkoituksena on edistää yrityksen ja sen henkilöstön vuorovaikutuksellisia yhteistoimintamenettelyjä, jotka perustuvat henkilöstölle oikea-aikaisesti annettuihin riittäviin tietoihin yrityksen tilasta ja sen suunnitelmista. Tavoitteena on, että yrityksessä kehitettäisiin yhteisymmärryksessä toimintaa sekä työntekijöiden mahdollisuuksia vaikuttaa päätöksiin, jotka koskevat heidän työtään, työolojaan ja asemaansa. (YTL 1 §.) Lakia yhteistoiminnasta yrityksissä sovelletaan yrityksiin, jonka työsuhteessa olevien työntekijöiden määrä säännöllisesti on vähintään 20 (YTL 2 §).

Yhteistoimintaneuvotteluissa on otettava huomioon yksityisyyden suojasta työelämässä annettu laki, jossa on säädetty tiedot, joita työnhakijasta ja työntekijästä saadaan kerätä, tietojen keräämisen edellytykset ja tietojen käyttö. Henkilöstön edustajat voivat myös yhteistoimintaneuvotteluissa esittää oman näkemyksensä kerättävistä henkilötiedoista ja niiden käsittelystä. (Lamponen 2016, 89.)

Yhteistoimintamenettelyssä osapuolina työnantaja sekä yrityksen henkilöstö. Paikalla voi olla myös työntekijän esimies taikka henkilöstöryhmän tai sen osan edustaja. (YTL 7 §.) Yhteistoimintavoitteen katsotaan täyttyneen, kun työnantaja on menetellyt yhteistoimintalaissa säädetyllä tavalla. Tällä tarkoitetaan, että työnantaja on antanut ennen neuvotteluja laissa säädetyt aloitteen ja tiedot (YTL 21 § ja 22 §) ja käsitellyt yhteistoimintaneuvotteluissa säädetyt asiat yhteistoiminnan hengessä yksimielisyyden saavuttamiseksi (YTL 19 § ja 20 §). Yhteistoimintalain 21 §:n mukaan aloitteen neuvotteluille tekee työnantaja. Myös henkilöstöryhmän edustajalla on aloiteoikeus. Tällöin työnantajan on tehtävä mahdollisimman pian aloite yhteistoimintaneuvottelujen käynnistämisestä. (YTL 23 §.)

Yhteistoimintaneuvotteluissa on käsiteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutettavan valvonnan tarkoitus, käyttöönotto ja käytettävät menetelmät, ennen valvonnan tai sen muutoksen käyttöönottoa. (Lamponen 2016, 95.) Työntekijöihin kohdistuvassa teknisin menetelmin toteutettavassa valvonnassa on mahdollista kerätä henkilötietoja, joten tällaista tilannetta koskee yhteistoimintalain 15§:n 3 kohta. Yhteistoimintaneuvotteluissa on sen mukaan käsiteltävä yrityksessä noudatettavat periaatteet, käytännöt työntekijöistä työhönotossa ja työsuhteen aikana kerättävistä tiedoista ottaen huomioon, mitä yksityisyyden suojasta työelämässä annetussa laissa säädetään.

Työnantajan on siis käsiteltävä paikantamisen perusteet, tavoitteet ja tarkoitukset, käytettävät menetelmät sekä käyttöönotto. Neuvotteluissa on käsiteltävä, miksi paikantamisen käyttöönottoa harkitaan, mitä sillä tavoitellaan ja miten asia vaikuttaa henkilöstöön. (YTL 19 ja 20 §.) Työpaikalla on myös tiedotettava työpaikalla paikannusjärjestelmän käytöstä siten, että kaikki työntekijät ovat tietoisia paikannuksen tarkoituksesta ja henkilötietojen käsittelystä sen yhteydessä. Läpinäkyvä informointi on yksi tietosuoja-asetuksessa mainituista perusperiaatteista. (Euroopan tietosuoja-asetus 12 art.)

Vaikka yhteistoimintalakia ei sovelleta alle 20 henkeä työllistäviin yrityksiin, on avoin ja selkeä informointi henkilötietojen keräämisestä ja käsittelystä tarpeen. Työnantajan on muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa ja julkisoikeudellisissa yhteisöissä aina ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista. (YksTL 21.1 §.) Henkilötietoja kerätessä muodostuu henkilötietorekisteri ja rekisterinpitäjänä

työnantaja on velvollinen huolehtimaan tietosuoja-asetuksessa säädettyjen rekisteröidyn oikeuksien toteutumisesta. Tietosuoja-asetusta ja rekisteröidyn oikeuksia on käsitelty aiemmin tässä opinnäytetyössä.

Yhteistoimintalain rangaistussäännöksen mukaan työnantaja tai tämän edustaja, joka tahallaan tai huolimattomuudesta jättää noudattamatta tai rikkoo, mitä kyseisessä laissa säädetään, on tuomitava yhteistoimintavelvoitteen rikkomisesta sakkoon. Vastuu työnantajan ja tämän edustajien kesken määräytyy rikoslaissa (39/1889) säädettyjen perusteiden mukaan. (YTL 67 §.)

## 6 TUTKIMUS

Opinnäytetyön tarkoituksena oli selvittää kuinka Euroopan yleinen tietosuoja-asetus vaikuttaa työntekijöiden paikantamiseen ja henkilötietojen keräämiseen, millaisia muita lainsäädännöllisiä haasteita paikantamiseen työpaikoilla voi liittyä ja millainen paikantaminen on ylipäättään työpaikalla mahdollista. Lisäksi tavoitteena on selvittää työntekijöiden suhtautumista paikantamiseen sekä työntekijöiden ja työnantajien saamia hyötyjä paikantamisratkaisusta.

### 6.1 Tutkimusmenetelmät

Opinnäytetyössä tutkimusmenetelmäksi valittiin kvalitatiivinen eli laadullinen tutkimus ja lainopillinen tutkimusmenetelmä. Lainopin keskeisin tehtävä on selvittää, mikä on voimassa olevan oikeuden sisältö käsiteltävässä oikeusongelmassa. Lainoppi pyrkii antamaan vastauksen kysymykseen, kuinka tilanteessa pitäisi toimia voimassa olevan oikeuden mukaan. Toinen lainopin tehtävistä on tutkimuskohteen systematisointi eli oikeuden jäsentäminen. Se auttaa löytämään etsityt säännökset sekä hahmottamaan kokonais kuvaa oikeudellisista järjestelyistä ja niiden välisistä suhteista. (Husa, Mutanen & Pohjolainen. 2001, 13-14.)

Opinnäytetyön lähteinä toimivat pääasiassa lait ja asetukset sekä niiden valmisteluaineisto. Lisäksi lähteinä käytettiin erilaisia viranomaisten antamia ohjeita ja raportteja. Näitä tutkimalla ja vertailemalla pyrittiin saamaan vastauksia siihen, kuinka Euroopan yleinen tietosuoja-asetus vaikuttaa työntekijöiden paikantamiseen ja henkilötietojen keräämiseen sekä millaisia lainsäädännöllisiä haasteita paikantamiseen voi ylipäättään liittyä.

### 6.2 Toteutus

Kvalitatiivinen eli laadullinen tutkimus toteutettiin teemahaastatteluin. Teemahaastattelussa haastattelu kohdistetaan tiettyihin teemoihin, joista keskustellaan. Haastattelu lähtee oletuksesta, että kaikkia yksilön kokemuksia, ajatuksia ja tunteita voidaan tutkia tällä menetelmällä. Teemahaastattelussa ei käytetä strukturoidulle lomakehaastattelulle ominaista kysymysten tarkkaa muotoa tai

järjestystä. Se ei kuitenkaan ole niin vapaamuotoinen kuin syvähaastattelu, jossa haastattelu muistuttavat hyvin paljon keskustelua. Tästä syystä teemahaastattelua voidaan kutsua puolistrukturoiduksi menetelmäksi. (Hirsjärvi & Hurme. 2001, 48).

Tämän opinnäytetyön haastattelujen tavoitteena oli selvittää työntekijöiden ja työnantajien suhtautumista paikantamisratkaisuihin, niihin liittyviin lainsäädännöllisiin haasteisiin sekä yksityisyyteen. Haastateltavaksi valittiin henkilöitä, jotka toimivat keskenään erilaisilla toimialoilla sekä erilaisissa tehtävissä ja rooleissa. Haastateltaviksi haluttiin kuitenkin valita henkilöitä, joilla on ennestään tietämystä paikannusratkaisuista, tietoturvasta tai henkilötietojen käsittelyyn liittyvästä lainsäädännöstä. Haastateltavien määrä rajattiin kuuteen henkilöön ja henkilöiden valinta perustui toimeksiantajan suosituksiin.

Teemahaastattelurunkoja laadittiin kaksi kappaletta (liite 1 ja liite 2), koska haastatteluissa tärkeää oli ottaa huomioon haastateltavan rooli työpaikalla. Työntekijöille suunnatun haastattelurungon keskeiset teemat olivat suhtautuminen paikantamiseen, yksityisyys sekä informointi henkilötietojen käsittelystä. Työnantajille suunnatussa haastattelurungossa keskeiset teemat olivat teknisen valvonnan nykytilanne yrityksessä, suhtautuminen paikantamiseen ja lainsäädännölliset haasteet.

Haastatteluissa keskustelu pyrittiin pitämään vapaamuotoisena, mutta kuitenkin ohjaamaan keskustelua haluttuun suuntaan käsiteltävien teemojen ja apukysymysten avulla. Erityisesti työntekijöiden osalta haluttiin saada selville työntekijöiden subjektiivisia kokemuksia siitä, kuinka he kokevat työnantajan suorittaman teknisen valvonnan.

### **6.3 Laaduntarkkailu ja luotettavuus**

Tutkimuksen laatua voidaan tavoitella tekemällä hyvä haastattelurunko sekä miettimällä, miten teemoja voidaan syventää. Lisäksi haastattelujen mahdollisimman nopea litterointi parantaa haastattelun laatua. (Hirsjärvi & Hurme. 2001, 184-185.) Tässä opinnäytetyössä haastattelurungot sekä apukysymykset käytiin läpi toimeksiantajan sekä opinnäytetyön ohjaajan kanssa ennen haastatteluiden toteuttamista. Näin pyrittiin varmistamaan, että haastatteluissa käsitellään toimeksiantajan kannalta tärkeitä teemoja. Haastatteluaineiston laadukkuus pyrittiin varmistamaan äänittämällä haastattelut ja litteroimalla ne mahdollisimman pian haastattelun jälkeen.

Reliaabeliudella tarkoitetaan perinteisesti sitä, että tutkittaessa samaa henkilöä kaksi kertaa saadaan sama tulos. Hirsjärvi ja Hurme toteavat kuitenkin kirjassaan, että reliaabelius koskee laadullisessa tutkimuksessa enemmänkin tutkijan toimintaa kuin haastateltavien vastauksia. Tällöin on tarkasteltava, onko kaikki käytettävissä oleva aineisto otettu huomioon, onko tiedot litteroitu oikein ja heijastavatko tulokset tutkittavien ajatusmaailmaa. Lisäksi aina on muistettava, että haastattelujen tulos on seurausta haastattelijan ja haastateltavan yhteistoiminnasta. (Hirsjärvi & Hurme. 2001. 186-189.) Validiteetti puolestaan ilmaisee, miten hyvin mittausmenetelmä mittaa juuri sitä, mitä sen on tarkoituskin mitata (Tilastokeskus 2018, viitattu 30.5.2018).

#### **6.4 Huoneentaulun suunnittelu ja toteutus**

Huoneentaulun (liite 3) toteutuksen lähtökohtana oli toimeksiantajan toive. Huoneentaulun tarkoituksena on havainnollistaa ja koota yhteen tärkeimpiä näkökulmia harkittaessa paikannusmenetelmien käyttöä työympäristössä. Tavoitteena on, että toimeksiantaja voi käyttää huoneentaulua tarjotessaan paikannusratkaisuja asiakkailleen.

Huoneentaulun suunnittelussa käytettiin hyödyksi tämän opinnäytetyön teoriapohjaa eli lainopillista tutkimusta. Keskeisessä roolissa on Euroopan tietosuoja-asetus sekä laki yksityisyyden suojasta työelämässä. Hyvänä apuna suunnittelussa toimivat myös teemahaastattelut. Haastattelujen yhteydessä huomattiin, että samat asiat nousivat esiin eri henkilöiden kanssa keskusteltaessa. Näiden voidaan katsovan olevan työntekijöiden näkemyksen mukaan erityisesti huomioitavia asioita paikannusratkaisuja harkittaessa. Erityisesti esiin nousivat paikannuksen pois kytkeminen vapaaajalla sekä avoin ja selkeä informointi.

Visuaaliselta ilmeeltään huoneentaulu pyrittiin pitämään toimeksiantajan toiveesta yksinkertaisena ja informatiivisena. Visualisoinnissa on käytetty apuna selainpohjaista grafiikka- ja kuvankäsittelyohjelmaa nimeltä Canva. Väreinä on käytetty toimeksiantajan brändin mukaista värimaailmaa ja ilmeen elävöittämiseksi neutraaleja kuvia.

## 7 TUTKIMUSTULOKSET

Haastateltavana oli yhteensä viisi henkilöä neljästä eri yrityksestä. Heistä neljä oli työntekijän roolissa ja yksi työnantajan roolissa.

Ensimmäisenä haastateltavana olivat Elfgroup Oy:n myyntijohtaja Kari Halavaara sekä toimitusjohtaja Tuomas Tonteri. Elfgroup Oy suomalainen sähköisten tietojen turvalliseen hallintaan erikoistunut yritys, joka tuottaa kyberturvallisuuden asiantuntijapalveluita ja pilvipalveluita yrityksille. Näitä ovat muun muassa tietoturvakonsultointi, hakkeritestaus, tietoturvallisten arkkitehtuurien kehittämisprojektit sekä yritysten kyberturvallisuusarvioinnit. (Tonteri & Halavaara, haastattelu 15.5.2018.) Halavaaran ja Tonterin haastattelu toteutettiin yhtä aikaa. Halavaara vastasi kysymyksiin työntekijän näkökulmasta ja Tonteri työnantajan näkökulmasta.

Tuomas Tonteri on Elfgroupin perustaja. Hän on valmistunut Oulun yliopistolta tietojenkäsittelytieteiden tiedekunnasta ja aiemmin toiminut muun muassa koodarina, ohjelmistoarkkitehtina sekä tietoturvakonsulttina. Työkokemusta häneltä löytyy niin F-Securelta kuin pankkialaltakin, jossa hän kehitti tietojärjestelmiä sekä verkkopalveluita.

Kari Halavaara on koulutukseltaan tuotantotalouden diplomi-insinööri. Pääaineena hänellä oli kansainvälinen markkinointi ja sivuaineena ohjelmistotekniikka. Halavaara on tehnyt pitkän uran Nokialla ja työskennellyt useissa muissakin yrityksissä ennen Elfgroupille tuloaan. Tällä hetkellä Halavaara vastaa Elfgroupin myynnistä ja markkinoinnista.

Kolmantena haastateltavana oli Testimate Oy:n Senior Quality Consultant Markus Kontturi. Kontturi on opiskellut tietotekniikkamekaniikkaa ja sen jälkeen ollut 16 vuotta Nokialla erilaisissa tehtävissä, joista viimeiset 11 vuotta tuotekehityksessä nimenomaan testauspuolella. Tällä hetkellä noin neljäkymmentäprosenttia työpäivistään Kontturi viettää Etelä-Suomessa asiakasrajapinnassa. Testimate Oy tarjoaa kokonaisvaltaisia ja riippumattomia ohjelmistojen testauspalveluita järjestelmähankkeisiin. (Kontturi, haastattelu 16.5.2018.)

Neljäntenä haastateltavana oli Transtech Oy:n tietojärjestelmäinsinööri Nemanja Vukota. Transtech on suomalainen kiskokalustotoimittaja ja konepajatuotteiden sopimusvalmistaja. Transtechilla on käynnistymässä kehitysprojekti, jossa Transtechin tuotteita lähdetään viemään uudelle



tasolle digitalisaation kautta ja yhtenä päätavoitteena on saada aikaan autonominen ajoneuvo. Tämä kehitysprojekti on Vukotan vastuulla. Vukota on koulutukseltaan diplomi-insinööri. (Vukota 17.5.2018, haastattelu.)

Viimeisenä haastateltavana oli Solita Oy:ssä business analytiikan konsulttina toimiva Jenni Linna. Solitalla hän on ollut töissä 10 vuotta ja koulutukseltaan hän on diplomi-insinööri. Käytännössä Linna työskentelee business intelligencen (liiketoimintatiedon hallinnan) käyttäjille näkyvän osuuden parissa (front end). Pääasiassa hän käyttää työssään erilaisia ohjelmistoja, kuten Cognosta, Tableautta, Birstiä, power BI:tä. Suuriosa työstä on tarvemäärittelyä, teknistä spesifiointia, raporttien tekoa sekä visualisoinnin tekemistä asiakkaille. Linnan työ on hyvin monipuolista ja riippuu pitkälti asiakkaan tarpeista. Linna on mukana Solitan IoT- tiimissä ja se kiinnostaa häntä kovasti.

## **7.1 Suhtautuminen tekniseen valvontaan ja paikantamiseen**

Ensimmäisenä haastatteluteemana oli työntekijän suhtautuminen työpaikalla tapahtuvaan tekniseen valvontaan. Ensimmäisen teeman yhteydessä käsiteltiin henkilöiden subjektiivisia kokemuksia ja tuntemuksia aiheeseen liittyen sekä suostumuksen antamista paikantamiseen.

Halavaaran mielestä esimerkiksi kulunvalvonta ja kameravalvonta työpaikoilla ovat täysin ymmärrettäviä teknisen valvonnan keinoja ja tärkeitä Elfgroupin kaltaisessa yrityksessä, jossa kyberturvallisuus on keskeisessä roolissa. Halavaaran suhtautuminen myös paikannusratkaisujen käyttöön työpaikalla on myönteinen ja hän olisi valmis antamaan suostumuksensa paikantamiseen. Paikantamisen pois kytkeminen olisi kuitenkin varmistettava työajan loputtua. (Tonteri & Halavaara, haastattelu 15.5.2018.)

Myös Kontturi kokee, että työpaikoilla tekninen valvonta on hyväksyttävää. Työnantajalla voi olla tiloissaan tietoa, laitteistoa tai jotain muuta jonka valvominen on tarpeen. Valvonta tulee kuitenkin olla rajattu niin, ettei sosiaalitiloja valvota. Kontturi ei suhtaudu myöskään paikantamiseen teknisen valvonnan menetelmänä kovin kriittisesti. Hän voisi nähdä paikantamisen jopa hyödylliseksi ainakin tietyillä aloilla. Esimerkkinä hän mainitsee rakennustyömaat ja muut työpaikat, joissa on korkea riski loukkaantua. Lähtökohtaisesti hän ei näkisi ongelmaa myöskään toimistoympäristössä tapahtuvassa paikantamisessa. Enemmän Kontturin mielestä herättäisi kummastusta se, jos työntekijä ei antaisi suostumustaan paikantamiseen työajallaan. Silloin herää hänen mukaansa epäily siitä,

että työntekijä käyttää työaikaansa jollain tapaa väärin. Kontturi tuo myös esille sen, että ihmiset jakavat nykyaikana vapaaehtoisesti itsestään sijaintitietoja esimerkiksi ystävilleen, joten hän ei näe ongelmaa työympäristössäkään. Kontturi kokee henkilökohtaisesti olevansa tässä mielessä helppo ihminen ja periaatteenaan hän pitää lausetta ”sen lauluja laulat, jonka leipää syöt”. Kontturi kuitenkin painottaa, että työntekijällä on aina voitava olla mahdollisuus kytkeä paikannus pois päältä työajan päätyttyä. (Kontturi, haastattelu 16.5.2018.)

Vukota suhtautuu tekniseen valvontaan positiivisesti siinä mielessä, että hän ei koe valvontaa häiritseväksi. Hän uskoo suhtautumisensa johtuvan koulutustaustastaan ja siitä, että tietää mihin kaiken tekniikan avulla pystytään ja miten suuri määrä dataa ihmisistä on jo kerätty. Vukota kuitenkin tiedostaa, että kaikki eivät varmasti ole asiasta samaa mieltä ja joidenkin suhtautuminen varsinkin työnantajan suorittamaan tekniseen valvontaan voi olla negatiivinen. Henkilökohtaisesti Vukota kuitenkin on sitä mieltä, että hänelle on yhdentekevää, valvotaanko häntä työajalla. Hän olisi valmis antamaan luvan paikantamiseen melkein missä vaan tilanteessa. Työnantajan tulisi kuitenkin perustella paikantaminen ensin. Ilman kunnollisia perusteluja Vukota ei antaisi lupaa. Työaikana Vukota sanoo olevansa työnantajan käytettävissä ja silloin hänen mielestään hänen ei kuuluisi tehdä asioita, joita hän ei voi työnantajalleen jakaa. (Vukota 17.5.2018, haastattelu.)

Linna kertoo työskentelevänsä todella vähän omalla toimistollaan ja teknisestä valvonnasta puhuttaessa pohtii työntekijöiden välille mahdollisesti syntyvää epätasa-arvoisuutta. Monet työntekijät tekevät nykyään töitä etänä tai asiakkaalla eikä työnantajalla tällöin ole samanlaisia mahdollisuuksia seurata heidän työskentelyään, kuin toimistolla työskentelevien työntekijöiden osalta. Linna ei koe työnantajan suorittamaa teknistä valvontaa negatiivisena asiana, jos henkilöt eivät ole yksilöitävissä. Esimerkkinä hän käyttää tilannetta, jossa työnantaja haluaa selvittää miten, erilaisia toimistotiloja hyödynnetään tai työnantaja haluaa varmistaa työntekijöidensä turvallisuutta valvonnan keinoin. Linnan mielestä valvonta on myöskin rajattava sosiaalitilojen ulkopuolelle. Oleellista hänen mielestään on myös se, että valvonnasta tiedotetaan työntekijöille avoimesti ja selkeästi. (Linna 23.5.2018, haastattelu.)

Myös Linna painotti, että suostumuksensa paikantamiseen hän olisi valmis antamaan vain tilanteessa, jossa työnantaja pystyisi hyvin perustelemaan, minkä takia paikantamista työpaikalla käytetään. Nykyisessä työssään Linna ei kuitenkaan näe mitään syytä, minkä takia työnantajan pitäisi häntä paikantaa. Hänen näkemyksensä mukaan aika on jo ajanut muun muassa kellokorttien käy-

töstä ohi eikä hän näe tarvetta edes sille, miksi työnantajan pitäisi seurata tarkasti toimistolla vietettyä aikaa. Toimistolla vietetty aika ei välttämättä kerro työn tehokkuudesta kovinkaan paljon ja lisäksi työtä tehdään hyvin usein asiakkaan luona. (Linna 23.5.2018, haastattelu.)

## **7.2 Paikantamisratkaisujen hyödyt ja haitat**

Paikannusratkaisujen hyödyistä puhuttaessa Halavaaran mielestä paikannusratkaisuja otettaessa käyttöön tulisi arvioida tarkasti siitä saatavia hyötyjä. Hän korostaa työntekijän ja työnantajan välistä luottamussuhdetta. Hänen mukaansa paikantamisen työpaikoilla tulisi aina perustua työnantajan ja työntekijän väliseen luottamukseen. Halavaara henkilökohtaisesti ei kokisi työnantajan suorittamaa paikantamista erityisesti yksityisyyttään loukkaavana. Halavaara voisi Elfgroupilla nähdä paikantamisesta hyötyjä vain tietyissä tilanteissa esimerkiksi palvelimien kaatumistilanteissa, jolloin voitaisiin nopeasti paikantaa lähimpänä oleva työntekijä, jolla on mahdollisuus korjata tilanne. Suurempia haittoja hän ei paikannusratkaisujen käytöstä näe aiheutuvan. (Tonteri & Halavaara 15.5.2018, haastattelu.)

Vukota puolestaan näkee, että paikannuksen avulla voitaisiin saada hyötyjä esimerkiksi teollisessa tehdasympäristössä työturvallisuuden osalta. Myös muu tekninen valvonta voisi olla hyödyksi. Esimerkiksi kameralla voitaisiin varmistaa, että henkilö on tehnyt tietyt työtehtävänsä oikein. Vukota kertoo, että esimerkiksi työtapaturman sattuessa työnantaja voi usein luottaa vain työntekijän sanoon. Tällöin voi olla hankala arvioida, onko työntekijä noudattanut työnantajan antamia työturvallisuusohjeita oikein vai ei. Poliisit tekevät tällaisista tilanteista tutkinnan ja se tekee usein työnantajan elämän hankalaksi, koska näyttöä suuntaan tai toiseen ei ole. Tiettyjen asioiden tarkkailu voisi siis Vukotan mukaan helpottaa hallinnollisia ja byrokraattisia toimenpiteitä yrityksissä. (Vukota 17.5.2018, haastattelu.)

Paikantamisen hyödyistä puhuttaessa Elfgroupin toimitusjohtaja Tonteri toteaa, että tietyillä toimialoilla paikantamisesta voitaisiin varmasti saada hyötyjä. Esimerkiksi logistiikkayhtiöissä parhaimman reitin suunnittelu voi olla keskitetty ja tällöin paikantaminen ja aikataulutukset voivat olla tarpeen. Elfgroupilla myyjät järjestävät pääsääntöisesti itse tapaamisensa asiakkaiden kanssa, eikä käytössä ole mitään keskitettyä systeemiä. Paikantamiselle Tonteri ei näe tarvetta tällä hetkellä Elfgroupilla, koska työ ei ole millään tavalla sijaintiriippuvaista. Mikäli työntekijä on asiakkaan luona, täytyy voida luottaa työntekijään. Halavaara otti esille keskustelun yhteydessä matkakulujen

automatisoinnin, jossa esimerkiksi kilometrimittareilla tai karttapiirturisovelluksilla voitaisiin helpottaa prosessia myös Elfgroupilla. Näitäkin jotkut henkilöt ovat omaehtoisesti Tonterin mukaan käyttäneet, mutta tällöin paikannustieto ei tule kuitenkaan työnantajalle. Tonteri toteaa, että esimerkiksi etäpäivien väärinkäyttöä epäillessä paikannus voisi olla kätevä myös toimistotyössä, mutta sellainen seuraaminen ei ole laillista. (Tonteri & Halavaara, haastattelu 15.5.2018.)

Tonteri uskoo, että toimiston ulkopuolella tapahtuva paikantaminen herättäisi varmasti työntekijöiden keskuudessa keskustelua ja kyseenalaistamista. Myös lainsäädännöllinen pykäliden tarkastelu luonnollisesti lisääntyisi työnantajan puolelta, mikäli paikannusratkaisuja ryhdyttäisiin käyttämään. Pykäliden tarkastelu lisääntyisi varmasti myös työntekijöiden keskuudessa, kun alkaisi spekulatio siitä, mihin dataa käytetään ja miten paikannuksen saa kytkettyä pois päältä. Työmäärää siis lisääntyisi paikantamisen käyttöönottovaiheessa varmasti, vaikka se myöhemmin hyötyjä toisikin. (Tonteri & Halavaara, haastattelu 15.5.2018.)

Kontturi uskoo, että paikantamisesta voi olla hyötyä suurissa yrityksissä joissa on paljon työntekijöitä. Esimerkiksi isoissa laboratorioissa työntekijöiden paikantaminen voisi olla hyödyksi tilanteissa, joissa työkaverin löytäminen nopeasti on tarpeen. Hänen mukaansa paikannuksesta voisi olla hyötyä myös yksilön oikeuksienkin kannalta. Tällainen tilanne voisi olla esimerkiksi testilaboratoriossa, jossa työntekijöiden pääsyä tiettyihin tiloihin on rajoitettu. Väärinkäyttötapauksissa työntekijät voisivat paikannusjärjestelmän avulla osoittaa, että he eivät ole liikkuneet alueella luvatta. Pienissä tiloissa työskennellessä Kontturi ei näe juurikaan paikannusratkaisulla saatuja hyötyjä tai perusteita paikantamiselle. (Kontturi, haastattelu 16.5.2019.)

Myöskään Vukota ei näe toimistoympäristössä paikantamisen hyötyjä kovin paljon. Ainoa hyöty jonka hän keksii ovat yleishyödylliset applikaatiot, joilla voitaisiin leikkiä ja seurata esimerkiksi mitä tiloja on käytössä mihinkin aikaan. Tätä kautta voitaisiin optimoida tilojen käyttöä. Toimiston tulisi kuitenkin olla hänen mukaansa melko suuri, koska pienissä toimistoissa tällaisille ei ehkä ole käyttöä. Pienemmissä tiloissa työntekijöiden seuraaminen sujuu ilman teknisiä apuvälineitä. Toimistyöntekijät voisivat kuitenkin hyödyntää paikannusratkaisuja esimerkiksi messutilanteista, joissa paikantaminen voisi auttaa löytämään henkilöitä messualueelta. Suunnistaminen alueella helpottuisi ja tiettyyn pisteeseen voisi etukäteen esimerkiksi sopia yhteistyökumppaneiden kanssa tapais-  
misiä. (Vukota 17.5.2018, haastattelu.)

Linnakaan ei näe toimistotyössä, jossa työnteko ei ole sidottu aikaan tai paikkaan, paikantamisratkaisuille kovin suurta hyötyä. Enemmän hyötyjä hän näkee tällaisille ratkaisuille käyttöä esimerkiksi kotisairaanhoidossa, jossa paikantamisratkaisun avulla voitaisiin varmistaa työntekijän turvallisuutta. Paikantamisen avulla voitaisiin esimerkiksi tarkkailla, kuinka kauan sairaanhoitaja asiakkaan luona viettää ja mikäli aika venyy tavanomaista pidemmäksi, voitaisiin helposti tarkistaa tilanne. (Linna 23.5.2018, haastattelu.)

Paikantamisratkaisujen käytöstä työpaikoilla voi Kontturin mukaan aiheutua myös haittoja. Hän uskoo, että tietyt ihmiset saattavat suhtautua paikantamiseen ja heidän seuraamiseensa erittäin negatiivisesti. Haittoja voi syntyä myös, jos tietoa käytetään väärin työnantajan toimesta. Tietojen käyttöä pitäisi valvoa siten, että määriteltäisiin tarkasti henkilöt, jotka tietoon pääsevät käsiksi. Paikantamista tulisi Kontturin mukaan käyttää vain etukäteen määritellyissä ja perustelluissa tilanteissa. (Kontturi, haastattelu 16.5.2018.) Myös Vukotan tuo esille, että paikannusratkaisuja työpaikoilla suunniteltaessa täytyy aina lähteä liikkeelle yksityisyys ja tietoturva edellä. Aina on huolehdittava siitä, että data pysyy työnantajan hallussa eikä siihen pääse ulkopuoliset käsiksi. Väärinkäytöksistä voi syntyä suuria haittoja varsinkin, jos sijaintitiedot ovat jollain tapaa olennaisesti integroitu kyseisen yrityksen toimintaan. (Vukota 17.5. 2018, haastattelu.)

Halavaara näkee ainoaksi haitaksi sen, että ihmiset usein kokevat tällaisten lisäävän ”isoveli valvoo” asennetta työpaikoilla. Halavaara painottaa, että työnantaja ei voi seurata työntekijää ihan vain seuraamisen ilosta, vaan paikantamiselle täytyy olla asialliset perusteet. (Tonteri & Halavaara, haastattelu 15.5.2018.) Samaa näkemystä toi esille Linna. Hän näkee suurimmaksi haitaksi paikannusratkaisujen käytöstä sen, että ne saattaisivat lisätä työpaikalla ”kyttämisen ilmapiiriä” ja uskoo tällaisen ilmapiirin vähentävän joustavuutta. Hänen mielestään valvontaa ei pitäisi käyttää vain valvonnan vuoksi, vaan jonkun perustellun syyn vuoksi. (Linna 23.5.2018, haastattelu.)

### **7.3 Yksityisyys**

Toisena haastatteluteemana oli yksityisyys. Yksityisyydestä puhuttaessa käsiteltiin erityisesti sitä, kuinka tärkeänä työntekijä kokee yksityisyytensä ja pystyykö hän mielestään vaikuttamaan siihen, millaista dataa hänestä ylipäättään kerätään. Keskustelu ei rajoittunut pelkästään datan keräämiseen työympäristössä vaan elämässä yleensä. Halavaara kokee olevansa kohtuullisen avoin ihmi-

nen ja pystyy samaistumaan jossain määrin väitteeseen ”henkilötietojen suoja ei ole minulle tärkeää, koska minulla ei ole mitään salattavaa.” Sosiaalisessa mediassa hän ei kuitenkaan jaa esimerkiksi lastensa kuvia eikä anna kaikille sivustoille lupaa käyttää laitteidensa sijaintitietoja. Halavaara kummastelee henkilöitä, jotka saarnaavat tietosuojan tärkeydestä, mutta kuitenkin jakavat kaiken itsestään ja perheestään sosiaalisessa mediassa. Hän kokee, että vastuu tiedon jakamisesta on ihmisellä itsellään ja ihmisen tulee voida päättää siitä, mitä tietoja hän haluaa itsestään julkaista. Tästä syystä esimerkiksi pienten lasten kuvien jakaminen ei ole hänestä sosiaalisessa mediassa järkevää. Halavaaran mukaan yksityisyys on joka tapauksessa tärkeä asia ja jokaisella tulee olla mahdollisuus hallita omia tietojaan. Siksi työntekijällä tulee jossain määrin olla oikeus suojata yksityisyytään myös työajalla esimerkiksi merkkamalla sähköisessä kalenterissa haluamansa merkinnät yksityiseksi. Saman pitäisi päteä myös paikantamisessa, mikäli sellaista käytetään. (Tonteri & Halavaara, haastattelu 15.5.2018.)

Kontturi puolestaan kokee yksityisyyden kahdelta kannalta. Omaa yksityiselämäänsä Kontturi ei halua jakaa kovin laajasti. Esimerkiksi puhelimelle tai tietokoneelle hän antaa vain harvoin luvan käyttää sijaintitietoja. Sosiaalisen median puolella hän on myöskin hyvin kriittinen eikä jaa esimerkiksi lasten kuvia tai tietoja profileissaan. Kontturi on kuitenkin sitä mieltä, että tällä hetkellä Android puhelimet rekisteröivät valtavan määrän tietoja ihmisistä. Hän kokee voivansa hallita hänestä kertyvää dataa vain jossain määrin teknologian asettamissa rajoissa. Teknologia asettaa rajoja sille, kuinka paljon ihminen voi pitää asioita salassa ja toisaalta myös sille, mitä tietoja on mahdollista kerätä. Kontturi pyrkii välttämään jakamasta tietoja, joiden keräämiselle hän ei näe asiallisia perusteita. (Kontturi, haastattelu 16.5.2018.)

Vukota kokee voivansa samaistua väitteeseen ”henkilötietojen suoja ei ole minulle tärkeää, koska minulla ei ole mitään salattavaa”. Hän kokee yksityisyytensä siinä mielessä tärkeäksi, että hän ei välttämättä edes haluaisi tietä, millä kaikilla tahoilla on hänestä mitään tietoa. Hän kokee olevansa hyvin tietoinen siitä mihin teknologialla nykyaikana pystyy. Tietyllä tapaa peli on hänen mielestään menetetty, koska nykymaailmassa ei ole enää kovin hankalaa saada haltuunsa haluamansa henkilön henkilötietoja. Vukota ei ole kovinkaan tarkka esimerkiksi puhelimensa sijaintitietojen käytöstä ja käyttää sosiaalista mediaa suhteellisen huolettomasti. Hän tuo esiin sen, että ihmiset saattavat somessa jakaa enemmän tietoa itsestään kuin uskovatkaan. Esimerkiksi pelkästään kuvia analysoimalla voi saada selville ihmisen sijaintitietoja. Oma dataansa voi Vukotan mukaan ensisijaisesti pyrkiä hallitsemaan tarkkailemalla, mitä itsestään jakaa sosiaalisessa mediassa. Tietenkin myös omaa selainkäyttäytymistään olisi hyvä tarkkailla, mikäli haluaa vähentää kertyvää dataa. Tämä

tarkoittaa esimerkiksi salatun selailun käyttämistä ja tietokoneen tai puhelimen sijaintitietojen käytön rajoittamista. Tärkeää on myös palveluiden käyttöehtojen huolellinen lukeminen. Hän kuitenkin myöntää, ettei usein jaksakaan käydä pitkiä käyttöehtoja itsekään läpi. (Vukota 17.5.2018, haastattelu.)

Linna ei pysty täysin samaistumaan väitteeseen ”henkilötietojen suoja ei ole minulle tärkeää koska minulla ei ole mitään salattavaa”, vaikka hänen mielestään hänellä ei ole mitään salattavaa. Hän haluaa pitää tietyt tiedot itsestään salassa välttääkseen esimerkiksi identiteettivarkaudet tai muut henkilötietojen väärinkäytökset. Nykyään Linna jakaa itsestään todella vähän tietoja esimerkiksi sosiaalisessa mediassa. Tähän on vaikuttanut hänen mukaansa lapsen syntyminen, koska hän ei halua jakaa mitään lapsestaan sosiaalisessa mediassa. Linna haluaa antaa lapselleen mahdollisuuden itse myöhemmin päättää siitä, mitä tietoja hänestä on saatavilla. Lapsi on kuitenkin luonnollisesti suuressa roolissa Linnan arjessa ja sen takia hänen syntymänsä on rajoittanut myöskin Linnan sosiaalisen median käyttöä. (Linna 23.5.2018, haastattelu.)

Linna ei myöskään anna internetsivuille kovin helposti lupaa käyttää sijaintitietojaan. Hän kokee syynä olevan tietynlaisen sisäänrakennetun varovaisuuden. Linna ei koe saavansa tarpeeksi suurta hyötyä esimerkiksi siitä, että Iltasanomat hakee valmiiksi hänelle säätiedot sijainnin perusteella. (Linna 23.5.2018, haastattelu.)

#### **7.4 Informointi**

Kolmantena haastatteluteemana oli informointi. Tämän teeman yhteydessä keskusteltiin, kuinka hyvin työntekijät ovat tutustuneet lainsäädännön näkökulmasta siihen, millaista teknistä valvontaa työnantajan on mahdollista käyttää ja miten työntekijöitä on informoitu valvontamenetelmien käytöstä. Työnantajan roolissa olevien kanssa keskusteltiin myös siitä, miten informointi on yrityksessä hoidettu.

Halavaara on mukana työryhmässä, jossa on selvitetty Elfgroupin henkilötietojen käsittelyä ja tästä syystä hän kokee tulleen työntekijänä hyvin informoiduksi siitä, mitä valvonta menetelmiä työnantaja käyttää ja miten henkilötietoja käsitellään. Tarkoituksena on, että koko yrityksen henkilöstöä informoidaan työryhmän selvittämistä asioista. Tonterin mukaan uuden työntekijän kanssa valvontaan liittyviä asioita ei käydä mitenkään erityisesti läpi. Elfgroup on noin 15 hengen yritys, joten

porukkaa on tullut pikkuhiljaa ja perehdytys on tapahtunut tähän asti tilanteen mukaan ilman varsinaista perehdytysprosessia. Yrityksen intranetistä löytyy kameravalvonnan rekisteriseloste ja sieltä asiat löytyvät, mutta asiasta informointi ei varsinaisesti kuulu säännönmukaiseen prosessiin. (Tonteri & Halavaara, haastattelu 15.5.2018.)

Työnantajan suorittamaa teknistä valvontaa ei käydä läpi säännöllisesti Elfgroupilla esimerkiksi kuukausipalavereissa. Tonteri näkee asian niin, että IT-alan asiantuntijoina kaikki työntekijät lähtökohtaisesti ymmärtävät, että periaatteessa kaikki mitä verkoissa liikkuu ja koneilla tehdään, on nähtävissä. Hän uskoo kaikkien myös ymmärtävän, että työpaikka on tietyllä tapaa kontrolloitu ympäristö. Tonteri kuitenkin totesi, että työntekijöiden valvonnasta informointia voitaisiin Elfgroupilla silti jollain tapaa selkeyttää. Elfgroupilla ei ole käytössä tällä hetkellä kameravalvonnan ja kulunvalvonnan lisäksi muuta teknistä valvontaa. Tonterin mukaan kuitenkin esimerkiksi aikaleimoja tallentuu paljon ja periaatteessa olisi mahdollista nähdä missä Wi-Fi tukiasemassa työntekijät ovat milloinkin kiinni. Tällaisen verkkoliikenteen seuraaminen on myös säänneltyä ja Tonteri otti haastattelussa esiin yhteistoimintaneuvottelut. Verkkoliikenteen seuranta tulisi käydä läpi yhteistoimintaneuvotteluissa, mikäli työntekijöiden verkkoliikennettä seurataan. Elfgroup on kuitenkin sen verran pieni yritys, että yhteistoimintaneuvotteluvuoroitusta ei ole. (Tonteri & Halavaara, haastattelu 15.5.2018.)

Kontturille taas on asiakastöissään sopimuksen tekovaiheessa selvennetty teknisen valvonnan käytännöt ja hän kokee tulleen hyvin informoiduksi. Peruskäytännöt ovat hänen mukaansa lähes poikkeuksetta samat asiakkaasta riippumatta, mutta joitain pieniä eroja saattaa valvonnan suhteen olla. (Kontturi, haastattelu 16.5.2018.)

Vukota uskoo, että hänellä on jonkinlainen käsitys siitä millaista valvontaa työnantaja saa käyttää työpaikalla. Hän ei kuitenkaan ole törmännyt tilanteisiin, joissa häntä olisi työpaikalla erityisesti informoitu valvontamenetelmien käytöstä. Hänen työpaikoillaan ei ole ollut juurikaan esimerkiksi kameravalvontaa. Kulunvalvontamenetelmät on käyty läpi, mutta niitä hän pitää niin itsestään selvänä, että ihmiset varmasti ymmärtävät näiden tietojen tallentuvan jonnekin. (Vukota 17.5.2018, haastattelu.)

Vukota on sitä mieltä, että työnantajalla pitäisi olla paremmat mahdollisuudet tarkkailla työntekijöitä. Työntekijöiden tarkemmalla tarkkailulla olisi mahdollisuus optimoida ja tehostaa työntekijöiden työntekoa sekä parantaa jopa työoloja. Hänen mukaansa ihmisten olisi hyvä lopettaa työnantajan



ja työntekijän vastakkainasettelu ja muistaa, että työnantajallakin voi olla intressi parantaa molempien osapuolten oloja. Tällaista vastakkainasettelua ihmisten mielissä hän on havainnut erityisesti teollisilla aloilla. Työntekijöille olisi hyvä saada tarkennettua, ettei työntekijöitä haluta valvoa valvomisen takia, vaan halutaan valvoa työtapoja, menetelmiä ja ympäristöä. (Vukota 17.5.2018, haastattelu.)

Linna ei enää muista tarkalleen minkälainen hänen perehdytyksensä Solitalle tullessa on ollut ja Solitan perehdytyskäytännöt ovat siitä muuttuneet hyvin paljon. Hän ei ainakaan muista, että teknisen valvonnan käytöstä olisi erityisesti keskusteltu. Hän uskoo, että tietosuoja-asetuksen myötä asioista aletaan systemaattisemmin informoimaan ja keskustelemaan. (Linna 23.5.2018, haastattelu.)

## **7.5 Paikantamiseen liittyvä lainsäädäntö**

Paikantamiseen liittyvää lainsäädäntö oli otettu varsinaiseksi haastatteluteemaksi ainoastaan työnantajille suunnatussa haastattelurungossa, mutta lainsäädäntö ja erityisesti tietosuoja-asetus tuli esille jokaisen haastattelun yhteydessä.

Kuten aiemmin jo haastattelussa tuli ilmi, Euroopan tietosuoja-asetukseen on Elfgroupilla valmistauduttu perustamalla sitä varten erillinen työryhmä. Työryhmä on tehnyt henkilötietoinventaarion. Tämä tarkoittaa, että on tunnistettu mitä henkilötietoja käsitellään, millä käsittelyperusteella, missä tietoja säilytetään, ketkä ulkoiset tahot tietoja käsittelevät ja missä tietojärjestelmät maantieteellisesti sijaitsevat. Tämän selvitystyön johdosta Elfgroupilla on esimerkiksi luovuttu entisestä asiakkuudenhallintajärjestelmästä, koska järjestelmän tiedot eivät pysyneet pelkästään EU- tai ETA-alueen sisäpuolella. Asiakkuudenhallintajärjestelmä vaihdettiin sisäiseen omilla palvelimilla olevaan järjestelmään. Lisäksi Elfgroupin rekisteriselosteita on päivitetty ja valmisteltu käytäntöjä, miten toimitaan, jos joku asiakas haluaa tietoonsa hänestä kerätyt tiedot tai poistaa ne. (Tonteri & Halavaara 15.5.2018, haastattelu.)

Tietosuoja-asetuksen positiivisina puolina Halavaara näkee sen, että yrityksissä saadaan parempi käsitys siitä, mitä dataa oikeasti kerätään ja mihin se tallennetaan. Prosessi kokonaisuutena hahmottuu paremmin ja samalla tulee mietittyä, mitkä tiedot ovat oikeasti tarpeellisia. Halavaara toi kuitenkin esille, että moni pk-sektorin yrittäjä tuskailee asetuksen voimaantulon kanssa edelleen.

Viranomaisten ohjeet ovat osittain sekavia. Riittävä henkilötietojen suojauksen taso on myös jätetty rekisterinpitäjän itsensä määriteltäväksi ja määrittely voi usein olla haasteellista. Tietosuoja-asetus voi hänen mukaansa tuntua monen mielestä byrokraattisemmalta asialta kuin se oikeasti onkaan. Lisäksi Halavaara on kuullut, että asetukseen on valmistauduttu eri puolilla Eurooppaa hyvin erilaisella asenteella. Etelä-eurooppalaisten valmistautuminen asetukseen on huomattavasti rennompaa kuin Suomessa. Asiaa on otettu Suomessa jo etukäteen paljon vakavammin ja siihen on valmistauduttu monissa yrityksissä jo pitkään. Tonterin mielestä ajatus tietosuoja-asetuksen takana on hyvä eikä siinä sinänsä ole kovin paljon mitään uutta. Henkilötietojahan on käsitelty ja säännelty aiemminkin. Asetuksen sovellettavaksi tulo on saatu hyvin tietoon ja harvasta asetuksesta tai laista on näin paljon syntynyt keskustelua. (Tonteri & Halavaara, haastattelu 15.5.2018.)

Halavaaran ja Tonterin kanssa samoilla linjoilla on myös Kontturi. Tietosuoja-asetuksesta keskustellessa Kontturi ottaa esille sen ympärillä olevan turhan ”pölinän”. Kontturin mukaan osa ihmisistä ottaa kaiken todella kirjaimellisesti, kun taas toisille tietosuoja-asetus ei merkitse yhtään mitään. Suhtautuminen asetuksen tuloon tuntuu Kontturin mukaan siis vaihtelevan hyvin paljon. Kontturi ei itse näe asetuksen tuovan kovinkaan paljon uutta. Pääpiirteissään tietosuoja-asetuksessa olevat artikkelit ovat samat kuin aikaisemmassakin lainsäädännössä olevat säännökset eikä asia sinänsä Kontturin näkemyksen mukaan muutu. Sanktiot kovenevat ja yksilön mahdollisuus hallita omia tietojaan paranee. Kontturin mielestä jo aiemmin olisi jo pitänyt olla järjestelmät, jotka seuraavat esimerkiksi sitä kuka käy katsomassa potilasrekistereiden tietoja. (Kontturi, haastattelu 16.5.2018.) Samaa mieltä on myös Vukota. Hän uskoo, että ihmiset heräävät ensimmäisen kerran siinä vaiheessa miettimään henkilötietojen suojaan ja yksityisyyteen liittyviä asioita tarkemmin, kun heidän tietojensa väärinkäytöllä saadaan aikaan jotakin oikeasti haitallista. Esimerkkinä tällaisesta haitallisesta väärinkäytöstä Vukota käytti hiljattain syntynyttä Facebook kohua. Kymmenien miljoonien amerikkalaisten Facebook-käyttäjien tietoja käytettiin ennustamaan Yhdysvaltojen presidentinvaalien tulosta. Tietojen kerääjänä toimi Cambridge Analytica -yhtiö. Tietojen avulla yhtiö kehitti ohjelman, jolla voitiin profiloida äänestäjiä. Tiedot kerättiin thisisyourdigitalife-sovelluksen avulla, jota on alun perin käytetty persoonallisuustesteissä. Cambridge Analytica kiisti kuitenkin syyllistyneensä väärinkäyttöksiin. (Uosukainen 2018.)

Vukotan näkemyksen mukaan tietosuoja-asetus tulee kuitenkin varmasti rauhoittamaan ihmisten mieliä, kunhan he ymmärtävät mitä se oikeasti merkitsee. Useimmilla ei vielä ole asiasta kovin

tarkkaa käsitystä ja se tuntuu aiheuttavan paljon huolta ja pelkoa. Vukota muistuttaa, että tietosuoja-asetuksen perimmäisenä tarkoituksena on tuoda ihmisille paremmat valmiudet hallita omia tietojaan eikä hankaloittaa tai hidastaa yritysten toimintaa. (Vukota 17.5.2018, haastattelu.)

Tietosuoja-asetukseen valmistautuminen on tuonut Vukotalle työssään eteen monia haasteellisia tilanteita. Useat asiat ovat viivästyneet ihmisten tietämättömyyden takia. Monia yksinkertaisiakin asioita kierrätetään yritysten lakiosaston kautta, koska tietämys asetuksen sisällöstä on heikko. Ketterät menetelmät menettävät helposti ketterän luonteensa tämän takia. Vukota uskoo, että jos ihmiset tuntisivat aiheen paremmin, he uskaltaisivat tehdä päätöksiä asioista nopeammin. (Vukota 17.5.2018, haastattelu.)

Myös Vukota on havainnut, että tietosuoja-asetukseen liittyvät konsultti- ja koulutuspalvelut ovat viimeisen vuoden aikana lisääntyneet merkittävästi. Hän kummastelee hieman sitä, miten asetuksesta on noussut näin iso juttu. Erilaisia lakeja, asetuksia ja direktiivejä tulee jatkuvasti, mutta harva niistä herättää näin paljon keskustelua. Vukota toivoisi, että yritysten päättävissä rooleissa olevat henkilöt tutustuisivat asetuksen sisältöön hyvin, jotta asioista ei syntyisi turhia byrokraattisia haasteita. Tällä hetkellä vai pieni joukko ymmärtää, mistä oikeasti on kyse. (Vukota 17.5.2018, haastattelu.) Samaa näkökulmaa toi esille myös Kontturi. Hänen mielestä on hyvä, että tietosuoja-asetuksen myötä pelisäännöt henkilötietojen käsittelystä muuttuvat selkeämmiksi, mutta tietosuoja-asetuksen ympärillä ollut ”hulabaloo” on hänen mielestään ollut jossain määrin turhaa. Konsultit ja lakimiehet ovat voineet myydä kaikenlaisia koulutuksia, jotka eivät loppujen lopuksi auta yritystä valmistautumaan asetuksen voimaantuloon. Koulutusten anti on Kontturin kokemuksen mukaan vain harvoin ollut niin hyvää, että sen jälkeen ihmisillä olisi ollut tiedossa, miten heidän tulee toimia. Kontturi on törmännyt omasta mielestään vain yhteen hyvään koulutukseen, jossa selkeästi kerrottiin mitä tietosuoja-asetus tarkoittaa. (Kontturi, haastattelu 16.5.2018.)

Linnan näkemyksen mukaan tietosuoja-asetus tuo tarvittavaa järjestystä ja selkeyttä henkilötietojen käsittelyyn. Hänen mielestään positiivista on erityisesti se, että jatkossa yksilöllä on parempi kontrolli omiin tietoihinsa ja paremmat mahdollisuudet selvittää, mihin kaikkialle henkilötietoja hänestä on tallentunut. Asetus tuo Linnan mielestä mukanaan paljon lisää työtä, mutta työn tekeminen asian ympärillä jatkuu varmasti sovellettavaksi tulon jälkeenkin. (Linna 24.5.2018, haastattelu.)

## 8 JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tarkoituksena oli tutkia kuinka Euroopan yleinen tietosuoja-asetus vaikuttaa työntekijöiden paikantamiseen ja henkilötietojen keräämiseen, millaisia muita lainsäädännöllisiä haasteita paikantamiseen työpaikoilla voi liittyä ja millainen paikantaminen on ylipäätään työpäällä mahdollista. Lisäksi tavoitteena on selvittää työntekijöiden suhtautumista paikantamiseen sekä työntekijöiden ja työnantajien saamia hyötyjä paikantamisratkaisusta.

Ensin tarkastellaan kuinka Euroopan yleinen tietosuoja-asetus vaikuttaa työntekijöiden paikantamiseen ja henkilötietojen keräämiseen, koska paikantamisratkaisujen käyttöönottamisen mahdollisuus riippuu hyvin paljon voimassa olevasta lainsäädännöstä. Tietosuoja-asetusta tutkimalla selvisi, että tietosuoja-asetus ei ota kantaa varsinaisesti ihmisten paikantamiseen tai edes työelämän tietosuojaan. Asetus on kuitenkin keskeisessä asemassa, koska paikantamisratkaisuja käyttämällä saadaan kerättyä ihmisistä henkilötietoja. Tietosuoja-asetuksen sovellettavaksi tuloon on valmistauduttu yrityksissä selvittämällä henkilötietojen käsittelyä koskevia käytäntöjä sekä dokumentoimalla niitä asetuksen vaatimusten mukaisesti. Mikäli työnantaja harkitsee paikannusratkaisujen käyttöönottamista, on tehtävä huolellinen arviointi siitä, onko paikantamiselle olemassa riittävät perusteet. Mikäli paikannusratkaisun käyttöönottamiseen päädytään, on huolehdittava riittävästä tietoturvasta sekä määriteltävä kenellä kaikilla on pääsy kertyviin henkilötietoihin. Tämän lisäksi asetuksen mukaisesta dokumentoinnista ja tiedottamisesta on huolehdittava.

Haastattelujen yhteydessä kävi selkeästi ilmi, että Euroopan tietosuoja-asetus on aiheuttanut yrityksissä lisätyötä, kouluttautumistarpeita ja asioihin perehtymistä. Haastateltavat kokivat asetuksen lainsäädäntöä selkeyttävänä tekijänä, mutta kritisoivat sen ympärille muodostunutta epäselvyyden ilmapiiriä ja tietynlaista pelkoa. Yksi haastateltavista kertoi asetuksen vaikuttaneen ketteriin menelmiin negatiivisesti ja hidastaneen prosesseja. Paikannusratkaisuja ei opinnäytetyön kirjoittamishetkellä käytetä vielä kovinkaan paljon työpaikoilla eikä henkilötietojen käsittelyyn liittyvä tietämättömyys ja epävarmuus varmastikaan kannusta harkitsemaan uusia ratkaisuja yrityksissä. Tilanne tulee todennäköisesti helpottumaan kansallisen lainsäädännön tarkentuessa ja mahdollisten oikeustapausten myötä.

Lainsäädäntöä tutkimalla voidaan todeta, että työntekijän paikantaminen on mahdollista vain poikkeuksellisesti ja se edellyttää aina työntekijän suostumusta. Opinnäytetyön tavoitteena oli lisäksi

selvittää työntekijöiden suhtautumista paikantamiseen. Suhtautuminen paikantamiseen on hyvin läheisessä yhteydessä suostumuksen antamiseen. Paikantamiseen myönteisesti suhtautuva työntekijä todennäköisemmin antaa suostumuksensa kuin negatiivisesti suhtautuva. Haastatteluista kävi ilmi, että työntekijät suhtautuvat melko neutraalisti työnantajan suorittamaan tekniseen valvontaan, mikäli siihen on asialliset perusteet. Työntekijät suhtautuvat paikantamiseen hyvin samalla tavalla kuin muuhunkin tekniseen valvontaan eivätkä pääsääntöisesti näe syytä, miksi eivät antaisi paikantamiseen suostumusta, jos siitä on saatavissa selkeitä hyötyjä.

Kaikki haastateltavat kokivat, että paikannusratkaisusta voisi olla hyötyä ensisijaisesti tehtaissa, laboratorioissa tai työympäristöissä, joissa työturvallisuuden tarkkailu on erityisen tärkeää. Toimistoympäristössä saatavia hyötyjä varsinkaan pienissä toimistoissa ei juurikaan nähty. Saatavat hyödyt tuntuivat pieniltä ja haastateltavat uskoivat, että ne voitaisiin saavuttaa myös muilla keinoilla. Toisaalta paikannusratkaisulla ei nähty olevan merkittäviä haittojakaan. Suurimmiksi huolenaiheiksi nousi ”kyttäysilmapiirin” lisääntyminen työpaikoilla sekä mahdolliset tietoturvaan liittyvät uhka- ja ongelmatilanteet.

Voidaan todeta, että paikannusratkaisujen käytölle ei ole työympäristössä lainsäädännöllistä estettä silloin, kun ratkaisun käyttö on perusteltua. Toimistoympäristössä työnantajan voi kuitenkin olla käytännössä lähes mahdotonta perustella paikannusratkaisujen käyttöä työturvallisuuteen liittyvillä seikoilla. Mikäli työnantajalla on tarve tai halu optimoida esimerkiksi tilojen käyttöä toimistossa, on hänen silti mahdollista hyödyntää paikannusratkaisuja. Tällöin työnantajan on saatava työntekijöiden suostumus paikantamisen käyttämiseen. Niiden työntekijöiden kohdalla, jotka eivät suostumustaan anna, paikantamista ei voida käyttää. Suostumukset on dokumentoitava ja työntekijöillä on oltava, milloin tahansa mahdollisuus peruuttaa suostumuksensa. Lisäksi asia on käsiteltävä yhteystoimintaneuvotteluissa, mikäli yrityksen työntekijöiden määrä on säännöllisesti vähintään 20.

## 9 POHDINTA

Opinnäytetyön tavoitteena oli selvittää työpaikoilla tapahtuvan paikantamisen lainsäädännöllisiä haasteita sekä työntekijöiden suhtautumista tekniseen valvontaan. Tavoitteena oli, että selvityksen avulla opinnäytetyön toimeksiantaja saisi tukea omaan toimintaansa tarjotessaan tai kehittäessään uusia paikantamiseen liittyviä ratkaisuja asiakkailleen. Tutkimus toteutettiin laadullisin sekä lainopillisin tutkimusmenetelmin. Lainsäädäntöä tarkastelemalla havaittiin, että lainsäädäntö on osittain puutteellista eikä lakeja säädettäessä ole osattu ottaa huomioon kaikilta osin viime vuosina tapahtunutta teknistä kehitystä. Haastattelujen avulla saatiin kartoitettua työntekijöiden suhtautumista tekniseen valvontaan työpaikoilla ja havaittiin, että työntekijöiden mielipiteet asiasta olivat hyvin saman suuntaiset. Tekninen valvonta, johon myös paikantaminen kuuluu, koettiin hyväksyttäväksi, mikäli työnantaja pystyy perustelemaan sen käytön riittävällä tavalla.

Mielestäni on ymmärrettävää, että lainsäädännöllä vain harvoin kyetään valmistautumaan ennakoon teknisen kehityksen tarpeisiin riittävällä tavalla. On kuitenkin harmillista huomata, että pahimmillaan ihmisten epävarmuus ja sekava ohjeistus voi johtaa tilanteisiin, joissa uusia menetelmiä ei uskalleta lähteä kokeilemaan ja kehittämään. Tällä hetkellä epävarmuus liittyy suurimmaksi osaksi tietosuoja-asetukseen eikä niinkään muuhun paikantamiseen liittyvään lainsäädäntöön. Tämä on ymmärrettävää, koska kyseessä on pitkä ja monitulkintainen asetus, johon useimmilla ei ole ollut aikaa riittävästi perehtyä. Epävarmuutta on mielestäni lisännyt se, että tietosuoja-asetuksesta tiedottaminen ja uutisointi on painottunut hyvin pitkälti mahdollisiin sanktioihin. Uutisoinnissa ei ole myöskään tuotu kovinkaan paljon esille sitä, että kyseessä ei suinkaan ole täysin uusi asia, vaan henkilötietojen käsittelyä on säännelty Suomessa tähänkin saakka.

Teemahaastatteluin pyrittiin selvittämään muun muassa sitä, millaisia hyötyjä työntekijät näkisivät paikannusratkaisujen käyttämiselle työympäristössään. Haastateltavat eivät juurikaan nähneet paikantamisella saavutettavia hyötyjä toimistoympäristössä ja olen heidän kanssaan samoilla linjoilla. Esimerkiksi tehdas- tai sairaalaympäristössä hyötyjä on saatavissa paikannusratkaisuin hyvin paljon. Uskon kuitenkin, että tulevaisuudessa hyötyjä havaitaan yhä enemmän ja paikannusratkaisut lisääntyvät myös toimistoympäristössä.

Oman näkemykseni mukaan opinnäytetyö vastaa sitä, mitä haluttiinkin tutkia. Validiteettia voidaan siis pitää hyvänä. Haastateltavien henkilöiden valinta oli onnistunut ja haastatteluilla saatiin vastauksia haluttuihin kysymyksiin. Opinnäytetyön aiheen rajausta muuttui ja eli prosessin aikana melko paljon, eikä liikkeelle lähdettäessä ollut tarkasti määriteltynä, millaista lopputulosta toimeksiantajan osalta tavoiteltiin. Lopputuloksena syntyi toimeksiantajan tarpeita vastaava selvitys sekä toiminnallisena osana paikantamiseen liittyvä huoneentaulu.

Haastateltavien joukko oli suhteellisen pieni ja haastateltavat edustavat hyvin samanlaista ammatikuntaa. Myös heidän koulutustaustansa olivat hyvin samankaltaiset, joten tutkimustulosta on hyvä arvioida kriittisesti. Toisaalta on otettava huomioon, että laadullisen tutkimuksen tarkoitus ei ole tavoitella yleistettävyyttä. Ihmisten suhtautuminen paikantamiseen voi vaihdella hyvin paljon, eikä ole mahdollista tehdä täydellistä yleistystä. Lisäksi on aina muistettava, että kyseessä on ihmisten subjektiiviset näkemykset, jotka voivat ajan kuluessa muuttua. Lisäksi uskon, että työntekijän ja työnantajan välinen suhde sekä työpaikalla vallitseva ilmapiiri vaikuttaa myös hyvin paljon siihen, miten työntekijät suhtautuvat tekniseen valvontaan. Mikäli työntekijän ja työnantajan suhde on hyvin etäinen, ilmapiiri kireä ja työntekijät kokevat jo ennestään olevansa tiukan tarkkailun alaisia, ei suostumusta lisätarkkailuun varmasti haluta antaa. Haastattelut antavat kuitenkin hyvän yleiskuvan siitä, millaisia asioita työntekijät pitävät tällä hetkellä tärkeinä suunniteltaessa paikantamisratkaisuja.

Koin opinnäytetyön tekemisen kaiken kaikkiaan mielenkiintoiseksi prosessiksi. Tietosuoja-asetukseen perehtymisen aloitin jo ammattiharjoittelua suorittaessani Solita Oy:ssä kesällä 2017. Lisäksi työni harjoittelun jälkeen on liittynyt suurilta osin tietosuojaan, jonka ansiosta noin vuoden ajan seurasin hyvin tiiviisti asetuksen sovellettavaksi tuloon valmistautumista yritysten näkökulmasta. Uskon tämän auttaneen suuresti kirjoitusprosessissa, koska kyseessä on melko laaja ja monitulkintainen asetus, johon perehtyminen ei tapahdu hetkessä. Aiheen ajankohtaisuus teki kirjoittamisesta mielekäästä, mutta toi mukanaan myös haasteita. Kuten johtopäätöksissä todettiin, lainsäädännön keinoin ei ole ennakoivasti pystytty vastaamaan kaikkiin teknisen kehityksen vaatimuksiin. Tästä johtuen aiheen tutkiminen vaati usean eri lähteen läpikäymistä, yhdistelyä ja tulkintaa. Lähdäaineistoa laajensi myös se, että aiheen kannalta oli tarpeellista perehtyä myös teolliseen internetiin ja paikannusratkaisujen toteuttamiseen liittyviin asioihin. Relevanttien ja luotettavien lähteiden valitseminen oli ajoittain haastavaa, koska lähteitä oli saatavilla valtavat määrät. Näistä valtaosa oli erilaisia ohjeita, artikkeleja, raportteja ja mietintöjä, joiden sisällöt saattoivat osittain poiketa

toisistaan tai eivät varsinaisesti vastanneet opinnäytetyön tutkimusongelmiin. Lisäksi oikeustapauksia liittyen työnantajan suorittamaan paikantamiseen oli hyvin haasteellista löytää. Mielestäni onnistuin kuitenkin hyvin lähdeaineiston rajaamisessa. Keskeisimmiksi lähteiksi muodostuivat Euroopan tietosuoja-asetus, laki yksityisyyden suojasta työelämässä sekä eri ministeriöiden antamat raportit ja ohjeet.

Kirjoittamisprosessin aikana elettiin myös niin sanottua siirtymäaikaa tietosuoja-asetuksen voimaantulon ja sovellettavaksi tulon välillä, joten oli erittäin tärkeää seurata asetuksen ympärillä tapahtuvia asioita. Myös uusi kansallinen tietosuojalaki oli kirjoittamishetkellä valmisteilla. Sen oli määrä tulla voimaan tietosuoja-asetuksen sovellettavaksi tullessa, mutta lain voimaan tulo kuitenkin viivästyi. Haasteita tuotti jonkin verran myös työn, opintojen ja opinnäytetyöprosessin yhteensovittaminen. Vaikka nämä kolme myös tukivat toisiaan, elämän aikatauluttaminen ja asioiden priorisointi tuottivat ajoittain haasteita. Kokonaisuudessaan voin kuitenkin todeta opinnäytetyön kirjoittamisen tuntuneen mielekkäältä.

Jatkotutkimusaiheita tälle opinnäytetyölle on löydettävissä useita. Paikantamista työelämässä on säännelty suhteellisen vähän ja tämän näkökulman jatkotutkiminen ei ehkä olisi kovin antoisaa. Jatkotutkimuksissa kiinnittäisin enemmän huomiota yleisesti ottaen henkilötietojen käsittelyyn, tallentamiseen ja hallintaan. Euroopan tietosuoja-asetuksen tavoitteena on ollut yhtenäistää henkilötietoja koskevaa sääntelyä sekä parantaa yritysten välistä kansainvälistä kaupankäyntiä. Mielenkiintoista mielestäni olisi tutkia, miten tietosuoja-asetus vaikuttaa uusien toimintatapojen kehittämiseen pidemmällä aikavälillä, parantaako se tosiasiasa yksilöiden mahdollisuuksia hallita omia tietojaan sekä miten yksityisyyden suoja otetaan huomioon lainsäädännöllisesti, kun verkkoon kytkettyjen laitteiden määrä edelleen lisääntyy.



## LÄHTEET

Alapuranen, L. 2016. Työntekijää koskevien henkilötietojen käsittelyedellytykset. Lapin yliopisto, oikeustieteellinen tiedekunta. Lisensiaatintutkimus. Viitattu 4.3.2018, file:///C:/Users/LocalAdmin/Downloads/Alapuranen.Leena.pdf.

Collin, J. & Saarelainen, A. 2016. Teollinen internet. Helsinki: Alma Talent.

Collin, J., Halén M., Juhanko J., Jurvansuu M., Koivisto R., Kortelainen H., Simons M., Tuominen a. & Uusitalo, T. 2015. Suomi - Teollisen Internetin Piilaakso. Helsinki: Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 4/2015.

Collin, J., Halén M., Juhanko J., Jurvansuu M., Koivisto R., Kortelainen H., Simons M., Tuominen Enroth, T & Neuvonen, R. 2017. EU:n tietosuoja-asetuksen yritysvaikutukset. Helsinki: Valtioneuvoston selvitys- ja tutkimustoiminnan artikkelisarja 10/2017.

EOA Dnro 1140/4/11

Euroopan ihmisoikeussopimus. Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi. 4.11.1950. (SopS 18-19/1990).

Euroopan perusoikeuskirja 2012/C 326/02

Euroopan tietosuoja-asetus. EPNAs (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (GDPR) 27.4.2016.

HE 125/2003 vp. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

HE 75/2000 vp. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi.

HE 9/2018 vp. Hallituksen esitys Eduskunnalle EU:n yleistä tietosuojaa-asetusta täydentäväksi lainsäädännöksi.

Heino, I. 2016. Yksityisyyden suoja ja luottamus liikkumisen sähköisissä palveluissa. Teknologian tutkimuskeskus VTT oy. Viitattu 4.3.2018, <http://www.vtt.fi/inf/pdf/technology/2016/T256.pdf>.

Henkilötietolaki 1999/523

Hirsjärvi S. & Hurme, H. 2001. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Husa, J., Mutanen A. & Pohjolainen, T. 2001. Kirjoitetaan Juridiikkaa. Helsinki: Talentum.

Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus ja siihen liittyvä valinnainen pöytäkirja yksilövalituksista. SopS 7–8/1976.

Kontturi, M. Senior Quality Consultant. Testmate Oy. 2018. Haastattelu 16.5.2018. Tekijän hallussa.

Korja, J. 2015. Yksityisyyden suoja työelämässä. Teoksessa: Niemi, M.-L. Oikeus tänään osa II. Kolmas uudistettu painos 2015. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 63.

Korja, J. 2016. Biometrinen tunnistaminen ja henkilötietojen suoja. Lapin yliopisto, oikeustieteellinen tiedekunta. Väitöskirja. Viitattu 23.4.2018, [http://lauda.ulapland.fi/bitstream/handle/10024/62397/Korja\\_Juhani\\_ActaE\\_193\\_pdfA.pdf?sequence=2&isAllowed=y](http://lauda.ulapland.fi/bitstream/handle/10024/62397/Korja_Juhani_ActaE_193_pdfA.pdf?sequence=2&isAllowed=y).

Korpisaari, P. Henkilötiedot ja paikkatiedot. Miten tietosuojalainsäädäntö vaikuttaa paikkatietojen julkaisemiseen ja luovuttamiseen. Ympäristöministeriön raportteja 10/2018. Helsinki: Ympäristöministeriö. Viitattu 26.4.2018, [https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160578/YMra\\_10\\_2018\\_Henkilotiedot\\_ja\\_paikkatiedot.pdf?sequence=1&isAllowed=y](https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160578/YMra_10_2018_Henkilotiedot_ja_paikkatiedot.pdf?sequence=1&isAllowed=y).

Laki paikkatietoinfrastruktuurista 421/2009

Laki sähköisen viestinnän palveluista 2014/917

Laki yhteistoiminnasta valtion virastoissa ja laitoksissa 1233/2013

Laki yhteistoiminnasta yrityksissä 2007/334

Laki yksityisyyden suojasta työelämässä 2004/759

Lamponen, H. 2016. Yhteistoimintalaki kommentaari. Helsinki: Alma Talent.

Lindgren, J. 2015. Teollinen internet – kuka omistaa tiedon? Asianajotoimisto Castrén & Snellman. Blogi & uutiset. Viitattu 6.5.2018, <https://www.castren.fi/fi/blogijauutiset/blogi-2015/teollinen-internet--kuka-omistaa-tiedon/>.

Lindroos-Hoviheimo, S. Lakimies 1/2018 s. 52–75

LiVL 6/2017 vp— U 19/2017 vp. Liikenne- ja viestintävaliokunnan lausunto. Viitattu 8.3.2018, [https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/LiVL\\_6+2017.pdf](https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/LiVL_6+2017.pdf).

Maanmittauslaitos 2017. Luonnos paikkatietopoliittiseksi selonteoksi, versio 0.8 / 22.9. 2017.

Oikeusministeriö 2017. Miten valmistautua EU:n tietosuoja-asetukseen. Oikeusministeriön julkaisu 4/2017. Helsinki: Oikeusministeriö. Viitattu 8.3.2018, [http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten\\_valmistautua\\_EUn\\_tietosuoja-asetukseen.pdf](http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf).

Patenttilaki 1967/550

Pervilä, M. 2013. Oma laite voi viedä yrityksen raastupaan. Tivi. Viitattu 23.3.2018, <https://www.tivi.fi/CIO/2013-04-24/Oma-laite-voi-vied%C3%A4-yrityksen-raastupaan-3200388.html>.

PeVM25 /1994. Perustuslakivaliokunnan mietintö n:o 25 hallituksen esityksestä perusoikeussäännösten muuttamisesta HE 309/1993 vp.

Rikoslaki 1889/39

Saarenpää, A. 2016. Oikeusinformatiikka. Teoksessa: Niemi, M.-L. Oikeus tänään. Osa I. Neljäs uudistettu painos 2016. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 64.

Saarenpää, A. Julkaisuvuosi ei tiedossa. Näkökulmia yksityisyyteen, tietoturvaan ja valvontaan. Lapin yliopisto, oikeusinformatiikan instituutti. Viitattu 22.3.2018, <https://www.ulapland.fi/loader.aspx?id=35185384-e21d-406b-96cc-1abe9705623d>

Suomen perustuslaki 1999/731

Tekijänoikeuslaki 1961/404

Tietosuojavaltuutettu dnro 87/41/2010.

Tietosuojavaltuutetun toimisto 2016. Kysymyksiä ja vastauksia. Viitattu 22.3.2018, <http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymysiajavastauksia.html>.

Tietosuojavaltuutetun toimisto 2018. Usein kysyttyä. Viitattu 22.5.2018, <https://tietosuoja.fi/useinkysyttya-tyoelama>.

Tilastokeskus 2018. Käsitteet. Viitattu 30.5.2018, <https://www.stat.fi/meta/kas/validiteetti.html>.

Tonteri, T. & Halavaara K. Elfgroup Oy. 2018. Haastattelu 15.5.2018. Tekijän hallussa.

Tuori, K. & Kotkas, T. 2016. Sosiaalioikeus. Helsinki: Alma Talent.

Työ- ja elinkeinoministeriö 2017. Suomen tekoälyaika – Suomi tekoälyn soveltamisen kärkimaaksi. Tavoite ja toimenpidesuosituksset. Työ- ja elinkeinoministeriön julkaisuja TEM raportteja 41/2017.

Uosukainen, S. 2018. Lehdet: Trumpin kampanjaan liitetty yhtiö keräsi tietoa salaa Facebookissa – kohteena 50 miljoonaa somekäyttäjää Yhdysvalloissa. Viitattu 23.5.2018, <https://yle.fi/uutiset/3-10121765>.

VAHTI-raportti 1/2016 – EU-tietosuojan kokonaisuudistus. 2016. Helsinki: Valtionvarainministeriö.

Valkjärvi, A. 2017. Henkilötietoja sisältävä tietokanta – konflikti immateriaalioikeuden hyödyntämisen ja henkilötietojen suojan välillä. Teoksessa Immateriaalioikeudet ja yleinen etu. Oesch, R., Eloranta, M., Heino, M. & Kokko M. 2017. Helsinki: Alma Talentum.

Valtioneuvoston kanslia 2017. Tietosuojalainsäädännön muutostarve, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017. Helsinki: Valtioneuvoston kanslia. Viitattu 26.4.2018, [http://tietokayttoon.fi/documents/10616/3866814/41\\_2017\\_Tietosuojas%C3%A4%C3%A4d%C3%B6sten+muutostarve/2c4ad983-8d90-480e-9b05-e3de9c9297c4?version=1.1](http://tietokayttoon.fi/documents/10616/3866814/41_2017_Tietosuojas%C3%A4%C3%A4d%C3%B6sten+muutostarve/2c4ad983-8d90-480e-9b05-e3de9c9297c4?version=1.1).

Valtionvarainministeriö 2017. Pilkahduksia tulevaisuuteen – digitalisaation ja robotisaation mahdollisuudet 10/2017. Helsinki: Valtionvarainministeriö. Viitattu 4.3.2018, [http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79260/Pilkahduksia\\_tulevaisuuteen.pdf?sequence=1](http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79260/Pilkahduksia_tulevaisuuteen.pdf?sequence=1).

Data Protection Working Party. Opinion 2/2017 on data processing at work. Viitattu 8.4.2018, <file:///C:/Users/LocalAdmin/Downloads/Opinion22017ondataprocessingatwork-wp249.pdf>

Vukota, N. Tietojärjestelmäinsinööri. Transtech Oy. 2018. Haastattelu 17.5.2018. Tekijän hallussa.

## HAASTATTELULOMAKE TYÖNTEKIJÖILLE

### Perustiedot

- Kuka olet, missä työskentelet, millaisissa työtehtävissä työskentelet, millainen on koulustaustasi?

### Teema 1 Suhtautuminen paikantamiseen

- Miten koet teknisen valvonnan työpaikalla? (Kulunvalvonta, kameravalvonta jne.)
- Antaisitko työnantajallesi suostumuksen paikantamiseen? Milloin antaisit, milloin et?
- Kokisitko paikantamisen yksityisyyttäsi loukkaavana? Miksi, miksi et?
- Millaisia hyötyjä/haittoja näet paikantamisratkaisujen käytössä työpaikoilla?

### Teema 2 Yksityisyys

- Kuinka tärkeäksi koet yksityisyytesi? Voitko samaistua väitteeseen ”henkilötietojen suoja ei ole minulle tärkeää, koska minulla ei ole mitään salattavaa?”
- Millä keinoilla pystyt mielestäsi vaikuttamaan siihen, millaista dataa sinusta kerätään?

### Teema 3 Informointi

- Oletko tutustunut lainsäädännön näkökulmasta siihen, millaisia valvontamenetelmiä työnantajan on mahdollista käyttää?
- Miten sinua on informoitu valvontamenetelmien käytöstä työpaikalla?
- Oletko muutoin tietoinen mitä työntekijöiden henkilötietoja työnantajasi käsittelee?

**Perustiedot**

- Kuka olet, missä työskentelet, millaisissa työtehtävissä työskentelet, millainen on koulutustaustasi?

**Teema 1 Nykytilanne**

- Millaisia teknisiä valvontamenetelmiä yrityksessänne on tällä hetkellä käytössä? (kamera-valvonta, kulunvalvonta jne.)
- Miten näistä menetelmistä on informoitu työntekijöitä?

**Teema 2 Suhtautuminen paikantamiseen**

- Voisitko harkita paikannusratkaisujen käyttöä työntekijöiden seuraamiseen työpaikalla? Miksi, miksi et?
- Miten luulet, että työntekijät suhtautuisivat paikantamiseen?
- Millaisia hyötyjä/haittoja näet paikantamisratkaisujen käytössä työpaikalla työnantajan näkökulmasta?
- Millaisia hyötyjä/haittoja näet paikantamisratkaisujen käytöstä työpaikalla työntekijän näkökulmasta?
- Voisiko paikannusratkaisuja mielestäsi käyttää esimerkiksi toimistoympäristössä?

**Teema 3 Lainsäädännölliset haasteet**

- Millaisia asioita työnantajan on mielestäsi otettava huomioon ennen paikannusratkaisujen käyttöönottamista?
- Miten lainsäädäntö rajoittaa paikannusratkaisujen käyttämistä työpaikoilla?
- Pitäisikö työnantajilla olla mielestäsi laajemmat oikeudet tarkkailla työntekijöitään?
- Kuinka Euroopan tietosuoja-asetus on otettu huomioon työntekijöiden henkilötietojen käsittelyssä?

## PAIKANTAMISEN ABC

Otettaessa paikannusratkaisuja käyttöön työpaikalla, on lainsäädännön huomioiminen tärkeää.



## SUOSTUMUS

Työntekijän paikantamiseen on aina pyydettävä suostumus.

## POIS KYTKEMINEN

Mikäli paikannusvälinettä on mahdollista kuljettaa mukana myös vapaa-ajalla, on varmistettava mahdollisuus kytkeä paikannus pois päältä.

## AVOIN JA SELKEÄ INFORMOINTI

Paikannusratkaisusta on aina informoitava työntekijöitä avoimesti ja selkeästi.



Työntekijällä on milloin tahansa oikeus peruuttaa suostumuksensa paikantamiseen.

